Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
US-APWR Subcommittee: Open Session

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, May 21, 2009

Work Order No.: NRC-2841 Pages 1-124

NEAL R. GROSS AND CO., INC.
Court Reporters and Transcribers
1323 Rhode Island Avenue, N.W.
Washington, D.C. 20005
(202) 234-4433

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

US-APWR SUBCOMMITTEE

+ + + + +

THURSDAY

MAY 21, 2009

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

OPEN SESSION

The Subcommittee met at the Nuclear Regulatory Commission, Two White Flint North, 11545 Rockville Pike, at 8:30 a.m., Dr. Otto L. Maynard, Chairman, presiding.

COMMITTEE MEMBERS PRESENT:

OTTO L. MAYNARD, Chairman
SAID ABDEL-KHALIK, Member
DENNIS C. BLEY, Member
CHARLES H. BROWN, JR., Member
JOHN D. SIEBER, Member
JOHN W. STETKAR, Member

ACRS STAFF PRESENT:

NEIL COLEMAN, Designated Federal Official

C-O-N-T-E-N-T-S

* Unintelligible due to Asian accent combined with technical terminology, hereafter referred to as

UDTAACWTT

P-R-O-C-E-E-D-I-N-G-S

(8:30 a.m.)

OPENING REMARKS

CHAIRMAN MAYNARD: Okay, I'd like to go ahead and call the meeting to order.

Good morning, everyone. I'm Otto Maynard, I'm chairman of the subcommittee for review of the topical report and SER for the diversity and defense in depth.

Mr. Neil Coleman of the ACR staff will be the designated federal representative for the initial portion of the meeting.

Members in attendance: We have Charles Brown, Dennis Bley, Said Abdel-Kahlik, John Stetkar, and John Seiber.

For people who have comments to make, especially if you're called from the audience to answer a question, I'd ask everyone to please come to a microphone. There are some on the desk and some up here, and speak into it and identify yourself.

The microphones are not for us to be able to hear. The microphones are actually for the transcription; the meeting is being transcribed, so that is the important part of that, and identifying yourself even if the rest of us know you, because the tape may not be able to see who you are.

I understand the purpose of today's meeting is to review the topical report and the staff's proposed SER relative to diversity and defense in depth for the USA-PWR.

It is also an informational brief on the gas turbine generator that Mr. Bissey is proposing for the US-APWR.

Relative to the topical report on diversity and defense in depth, I understand that the topical report was submitted in hopes of being able to use that for other operating plants. And I think the staff is going to talk a little bit about this. And it was -- the staff's review was limited to the US-APWR.

One of the things that I found just a little bit confusing, and I want the staff to address, and I think they have some answers to this, is that the SER identifies a number of application-specific action items, and yet the topical report is also limited to the US-APWR.

So I'd like just a little bit of

discussion as to why have application-specific action items in something that appears to be a topical report that is for an application-specific design.

So I've asked the staff to address that as part of their presentation.

The focus on today's meeting, we have kind of a mix. The primary focus is for the items in the SER that the staff is proposing to approve, and that we are going to be approving at our full committee meeting, and we will be making our comments on, recommendations yea or nay on. There are other parts like the gas turbine generator, and some of the application specific items in the SER that at this time we are not making any final conclusions on. So I'm going to be trying to focus the meeting on the things that we are really looking at for whether we agree or disagree on approving.

There is a chance that we can finish the meeting in one day. We do have time scheduled tomorrow morning, if we don't get finished today. It's all going to depend on how many questions we have, and I don't want to curtail the questions for that. But I will know better by noon or the middle of the afternoon where we stand on all that.

The beginning portion of the meeting is going to be open. We do have some closed sessions for some of the topics that we will be discussion, but we will be starting out in open session.

So with all that said, I'd like to turn it over to I think Carey to make some comments and get started.

MS. BICKETT: Good morning. My name is Carey Bickett, and I'm the acting chief for the US-APWR projects branch.

I just want to take a quick couple of minutes to say thanks to the committee for meeting with us today.

We have two short presentations prepared on the gas turbine generator and the defense in depth and diversity safety evaluation report.

And with that I'd like to turn it over to Ngola Otto.

INTRODUCTION TO (1) QUALIFICATION AND TEST PLAN OF CLASS 1E GAS TURBINE GENERATOR SYSTEM AND (2) SAFETY EVALUATION REPORT

MR. OTTO: Good morning, everyone. Good morning. I'd like to say thanks to the ACRS staff, and all the staff members here this morning.

I'm going to do be doing a quick overview of the gas turbine generator portion. And my name is Ngola Otto. I'm the chapter APM for the US-APWR design.

I've been involved with this part of the design for review.

The purpose of this presentation is we are going to provide the status of the NRC staff review of the US-APWR design, control document Chapter 8 and Chapter 9, Section 9.5 through 9.58. And we are going to be looking at the technical report that is referenced in the design control documents.

And also we are going to try to address any questions from the committee.

Gas turbine generator applicability, for the US-APWR designs we are using four gas turbine generators, safety related class 1E onsite power source, and for this design it is the first of its kind commercial use in nuclear power plants. So that is one of the things that is unique.

And also for the US-APWR design we have two gas turbine generators as alternate AC power sources. And also we are looking at the reliability related to the gas turbine generators meeting their reliability based on Reg Guide 1.155 of minimum 95 percent reliability.

And we are also looking at the diversity aspect of it to meet the Commission's guidance on the diversity problem of the AC power source. Next slide.

So far as part of the design review status we've issued RAIs, and we've received responses, both as it relates to Chapter 8 sections, and Chapter 9 sections. And we have had teleconference meetings, which were conducted back in March.

MEMBER BROWN: Can I ask one question? You say you are going to have four for safety related items, and then there is two for alternate AC. Are there six total, or are there just four?

MR. OTTO: Yes, six total.

MEMBER BROWN: Okay, that's fine, thank you.

MR. OTTO: And we've had teleconference meetings back in March to discuss Chapiter 8 related issues, and we also focused on the gas turbine generator.

The two things we focused on was the diversity and reliability of the gas turbine generators.

And MNI initiated a public meeting which we had on April the 13th to address the two issues, reliability and diversity, and from that meeting we -- our staff issued follow up RAIs to address those issues and other issues.

And we are planning to issue those RAIs soon within the coming weeks.

And MHI has -- are going to propose a diversity strategy for alternate DC source. They are planning to propose that to us based on our discussions in a public meeting. So that is still being worked on by MHI.

And based on our meeting it also -- MHI based on our RAI they are going to revise the report on this specific area based on the responses.

And as far as the GRG review, those will be included in Chapter 8 sections and Chapter

9 sections, safety valve issue report.

Next slide. And as a quick summary the design review is currently being conducted and MHI has decided to conduct a total of 100 initial type tests for IEEE 387 Section 6.2, which they have to meet the reliability requirements. And they are going to elaborate more on their testing climate as they do their presentation as far as how many tests and their reliability target that they are going to try to meet.

MEMBER BLEY: These will be tests of just the turbine generator with no loads attached or sequence going to it?

MR. OTTO: There are three or four types of test.

MEMBER BLEY: Within the 100?

MR. OTTO: Yes, there is -- I think MHI is probably going to --

CHAIRMAN MAYNARD: MHI is going to have a presentation on that, and maybe probably --

MEMBER BLEY: Okay, I was just wondering if staff had the whole plan. How that would be done. So you understand how they be loading the generators for the test?

MR. OTTO: We have the report, but we

don't have the full difficulties of the test. I know there are -- from what I see their size from Section 6.6.2 of IEEE 387, that it doesn't interfere.

MEMBER ABDEL-KHALIK: Now this is going to be one of the MSVI systems, versus the current plans. Have you thought this process through in terms of how you evaluate the status of this MSVI system in the reactor oversight process?

MR. OTTO: I am not. I could turn it over to one of our staff. Are any of you guys familiar with the process?

MR. GILL: My name is Paul Gill, and I'm with the electrical engineering branch involved in the review of the gas turbines.

At this stage we are, since there are no existing documents that address gas turbines, the only documents that are available are for the diesels. Reg Guide 1.9 and IEEE 387. And in those documents we have the requirements for the diesels, and essentially MHI has referenced those documents in their technical report for qualifying the gas turbines.

We are developing independently an interim staff guidance that also follows the guidance given in these documents, and that should be out sometime later.

In terms of the reactor oversight, I believe that MHI has not addressed that in their technical report. That is something that once we qualify the gas turbines, then it will fall into the reactor oversight program.

At this point we are not focusing on that. Our focus right now is to qualify the gas turbines so that they meet the minimum reliability requirement, or whatever reliability target MHI chooses for their gas turbines, and how they qualify it, and what the test plans are. You know this is a commercial grade. They are going to dedicate it commercially to class 1E before the do the 100 tests.

I don't know if that answers your question.

MEMBER ABDEL-KHALIK: I just want to make sure that you thought the process through.

MR. GILL: When you say reactor oversight I assume that it is going to fall similarly as we do for the diesels. Right now the big steps is, the goal I mentioned is a first-of-a-kind application for a nuclear power plant. So therefore we want to make sure that it meets all the requirements, off and onsite class 1E power source.

MEMBER ABDEL-KHALIK: My question is, correct me if I'm wrong, but part of the assignment of a color code to an MSI system depends on reliability data for other plants. And if this is a unique system, then how do you do that?

MR. GILL: Well, that is the issue we have been trying to put our arms around. The data that MHI provided to us for supporting the reliability fo these units is based on commercial units. And they vary in range from very small units to the sizes that are equivalent to what they are proposing to furnish. So it's very difficult to correlate that commercial data to a nuclear grade type components, and those are some of the issues that we have been going back and forth. And you have seen some of our RAIs on it questioning that data.

So the real proof is for them to do these 100 tests with no failures to arrive at a given reliability target that they choose, and we have been also bouncing back and forth how many tests they need. And I think finally we have come to the conclusion mutually, and that meets IEEE 387, that requires 100 tests, with no failures, and that includes start and run with load.

I think the question earlier was, whether they are going to load it or not. So we are going to follow that guidance in IEEE 387.

I don't know if that answers your question, but that is where we are. We are struggling to put our arms around this issue, because it's a first of a kind and we are concerned about it. We want to make sure that it has the same reliability achievements as the diesels do.

CHAIRMAN MAYNARD: I think Jack was first.

MEMBER SIEBER: I think you just made the point that I was going to bring up. Your expectation is to have the gas turbine generators as reliable as diesel generators, taking into account that because of the operation of the safety injection system they don't have to start and load as fast.

On the other hand the reliability should be the same as the expected reliability of the diesels. The more important factor is to assume now that -- or verify now that the gas turbine generators are suitable for this application without the reliability data for these specific models. And that is another issue, and that is what we are going to deal with today.

MR. GILL: Yes, and the staff has been dealing with that, and trying to arrive at a consensus with MHI as to what is the appropriate number of tests, and the type of test that they need to do. Before the staff buys into it.

MEMBER SIEBER: That is basically a statistical problem.

CHAIRMAN MAYNARD: And once the initial review and qualification is done isn't it going to be up to Mitsubishi and the COL proposed programs for what they do on an ongoing basis to monitor and to show that they are meeting the requirements there?

MR. CIOCCO: Correct.

MR. GILL: But certainly, once the gas turbine is qualified, then it will have to fall right into what the Reg Guide 1.155 calls for, a maintenance program to maintain that reliability target just like we do for the diesels today.

So the first step really, the big hurdle right now is to get it qualified.

CHAIRMAN MAYNARD: I would like to go ahead and move on.

MR. OTTO: Thank you.

OVERVIEW OF SAFETY EVALUATION

REPORT FOR MHI US-APWR

MR. CIOCCO: Good morning, my name is Jeff Ciocco. I'm the lead project manager for the US-APWR design certification.

I'm going to give you an overview this morning of our licensing review of this topical report, defense in depth and diversity.

This is a big milestone for us. We have been briefing you since October on our 12 topical reports. In October we did the fuel design and thermal hydraulics. In November we came to you with an informational brief with Mitsubishi, went over the four digital INC topical reports. And then in February up at the Pittsburgh offices of Mitsubishi, we briefed you on the four accident analysis topical reports. Those were all informational briefings.

Now we are coming to you, we have our

first safety evaluation report coming out. So I'm just going to give you an overview, and following my presentation is going to be Royce Beacom who is our INC engineer, digital INC engineer, who prepared the safety evaluation report.

So I'm going to give you an overview of this document. It's about a 75-page topical report. We are on revision two. I know that you are well familiar with it. Next slide.

Once again this is one of the four topical reports that we have related to the digital INC. The card, MUAP, goes from 07004 through 07007. This is 006, and these other three are currently in review. The safety system INC, the MELTAC. These are both related to Chapter 7, a reference in Chapter 7 of our design control document. Then we have the human factors engineering topical report. You had informational briefings on all three of those as well.

We are here today for the defense in depth and diversity. Mitsubishi requests approval of this topical report. It is referenced you will see in Chapter 7; it's probably referenced over 20 times in Chapter 7 for its defense in depth which is a process to minimize the potential for common cause failures in digital safety systems. Next slide.

What we have done in our licensing process to get us here, the first REG zero came to us in April, 2007. We conducted an acceptance review. This was back in the pre-application time of the US-APWR. We conducted a meeting in the summer of 2007. Mitsubishi revised their topical report in July of 2007. We then issued an acceptance letter which is actually -- I checked this morning -- this should be January of 2008.

And in that letter, and this gets to a point that we heard earlier that the committee wants the staff to address, is in that letter we said that we will not be doing this review for the operating fleet, and we made a reference to the NUREG 6303 which is the method of analysis for the AD3 because so many features vary amongst the plans. We dropped it off of its application to the current operation fleet.

And I think whenever Royce gets up and talks about the ASIAs, the application specific action items, we will address your question there.

But this letter was really what addressed where we are going to be applying this to the current operating fleet.

We had RAIs issued last year, and responses from Mitsubishi last fall. Like I said this was on November 4th and 5th, we gave you an informational briefing on all four topics on November 5th, was the D3 that Mitsubishi went in great detail on.

At that point we had a draft safety evaluation report prepared. It was sent to Mitsubishi which is what we do with all our topical reports whenever we have a draft SE, we send it to them to do an adequacy review and a proprietary determination.

That was in January of 2009, 2009 of this year. In March Mitsubishi responded. They had five comments in a publicly available letter that we were able to address.

So here we are today. We are going to present the draft safety evaluation report in both an open and a closed session. Royce is going to do that, and then we have been asked to come back I think on June 3rd, and present to the full committee I guess an abbreviated -- it's an hour, hour and a half meeting -- where we can come back and we will address any question that you have between now and then if we can, and we will come back to the full committee.

So this is an important point for us to conclude all of our informational briefings, and now we can start delivering the safety evaluation reports.

And then in summary we are ready to show you the evaluation findings on the defense in depth and diversity.

But that was all I had for my overview.

CHAIRMAN MAYNARD: Anytime we review a topical report that we are going to comment on, we need to have a session with the full committee. Because subcommittees do not issue letters or form conclusions on their own. It has to be for the full ACRS. So we will try to pick today at the end of the meetings thing we think we really need to focus on for the full committee meeting there.

MR. CIOCCO: That's great, and we are currently working on the schedules for our other topical reports and how they relate to our chapter completions. And I will work with Neil in getting the complete schedule.

CHAIRMAN MAYNARD: And just be advised, there will be probably a number of the same ones of us that will attend other topical reports, the ones that are thermal hydraulic specific and those will probably be reviewed by the thermal hydraulic subcommittee, and we will provide some continuity stuff with that, but those will fall into a different subcommittee.

MR. CIOCCO: I understand, okay, thank you.

MR. JACKSON: While Royce is getting started there, my name is Terry Jackson, and I'm the branch chief of instrumentation and controls and electrical engineering branch number one in the Office of New Reactors, and our branch was responsible for reviewing the MHI topical report on defense in depth and diversity, as well as other aspects of the US-APWR INC design.

And of course to my right here -- or to my left -- is Royce Beacom. He is a member of my staff and responsible for developing the safety evaluation report.

And just to keep in mind this topical report is not the full defense in depth and diversity analysis that is needed for the US-APWR application. There is also a coping analysis which is part of the US-APWR application that we are currently reviewing.

MEMBER STETKAR: I am glad you brought that up. Because I had written a note to myself. The SER has a lot of caveats in it, and references to several other topical reports. You just mentioned the coping analysis, but it also refers to the topical report on the digital platform itself, and the human systems interface, or HFE, human factors engineering topical report.

And I was curious as far as the staff is concerned, I have not been involved with the reviews of many of these topical reports, it seems difficult to approve in isolation a single topical report when it is actually integrally involved with a suite of topical reports, at least these four together.

How does that process work? How can you approve this one in isolation when indeed the approval may be contingent on your view and acceptance of other topical reports which you are then reviewing in isolation?

MR. JACKSON: Yes, I think the preventive topical reports that came in before the

US-APWR application came in, so the intent was to give the staff an early look at some of these issues and so forth. And from that perspective it provides an advantage.

But then again the challenge is when you have separate topical reports and they are integrated, how do we ensure that there is consistency among the topical reports and the final US-APWR application?

That is something that my staff has to look at, and I think you will see even in the SER there that in some cases we are saying that there is an application-specific action item contingent upon approval and another topical report for a particular component.

So we have to track those interdependencies between the topical report and the application, so for -- like I said if it were just a technical report it would be just one safety evaluation. But being a topical report it gets its own safety evaluation.

MEMBER STETKAR: But does the staff have any -- and this is a procedural question, not a technical question -- does the staff have any flexibility to bundle them together and issue a safety evaluation report on the group as a whole rather than for individual standalone safety evaluations that are somehow linked with a lot of bookkeeping.

MR. JACKSON: In some other applications we are actually looking at that, if the topical report is just applicable to a particular reactor design, we are communicating with the applicants and saying, hey, it may be better just to convert it to a technical report. Therefore it would just have one safety evaluation; that would be on the design certification application itself.

In this case we were pretty much complete with the D3 topical report for MHI, even though it is just for the US-APWR, and but some of the other like the safety system INC description and the MELTAC topical reports, MHI is requesting approval for current operating reactors also. So we can't write one -- it needs its own safety evaluation. So it does complicate matters, and where we can gain efficiencies by perhaps converting them to the technical reports we try to do that, but in some cases we can't.

CHAIRMAN MAYNARD: I do think this is

a little problematic from a bookkeeping standpoint, but I don't know that it needs to affect us right now for our reviews here. But where a topical report is actually referencing another topical report that hasn't been approved yet, what happens if that other topical report is changed in the review of that? It looks like it could end u being quite a bookkeeping nightmare.

MR. JACKSON: Right, and the resolution would actually be in the design certification application itself.

CHAIRMAN MAYNARD: That is true, but once a topical report is -- SER is issued, then that is kind of like a contract. The applicant has the ability to refer back and say, well, you approved that. So let's go on with the presentation. It' something I think we might need to have some more discussion on, is just a little bit of the complexity of approving topical reports that are relying on other topical reports that haven't been approved yet, and also where this one is application specific yet there are application-specific action items.

MR. JACKSON: And maybe I can try to address your one question about, why do we choose the term, application specific action item versus plant specific action item.

And when we looked at it we said, well, really, it is referring to the US-APWR design certification application, and we said, well it's not -- even though it's a design for a plant, it is not really a combined license application. So therefore we said, it's probably better to use application than plant in this case. We didn't really choose the term, because initially it was proposed for current operating reactors also.

But we deliberated on that shall we call it plant-specific action item and our application-specific action item. And we said, well, they both kind of do the same job; it's just the name that we give them. We thought application-specific action item would fit the US-APWR application better.

CHAIRMAN MAYNARD: Okay, so many of your application-specific action items might actually be a COL action item?

MR. JACKSON: What we envision is that in some cases some of the application specific cation items would be closed out in the

US-APWR design certification. They may provide whatever design information there.

In some cases some of the application-specific action items may actually be a verification item that would be an ITAAC in the design certification also.

So they could be potentially carried on, but changed into an ITAAC or combined license action, or COL action item.

CHAIRMAN MAYNARD: All right, let us go ahead and move on.

MR. BEACOM: All right, let me say personally, good morning, my name is Royce Beacom. I'm in the Instrumentation, Controls and Engineering branch of the Office of New Reactors. I've been in the ICE branches since the inception of the office of new reactors.

Before that, about a year and a half in operating reactors, and before that about 20 years with Westinghouse.

So I look forward to your comments. They always seem to be very insightful and helpful to the staff.

On the agenda, we are going to look at the background of this topical report, and the

SER, and how it fits generally into the US-APWR design certification and with the other topical reports.

We are going to look at the D3 scope for both the topical report and the SER; then the significant requirements standards and policies and guidelines that we use to review the topical reports.

We are going to look at the findings and conclusions. Then we are going to look at the application-specific action items.

Now as far as background as Jeff mentioned, these are the four topical reports. They are generic portions of the MHI digital INC design.

Now three of these are being reviewed by our branch with the exception of the HSI. They were initially reviewed by Oak Ridge National Labs for a technical engineering report that the staff took from there.

Now there is also as Jeff mentioned right now the D3 topical report and the SER is for a new reactor design only. That is the US-APWR. The MHI tech was for the operating fleet also.

Now in the acceptance letter the

Agency identified that particularly coming from the Office of Operating Reactors, that for the operating fleet the attributes of diversity are unique for each operating reactor, and therefore it will be difficult to apply a generic topical report for defense --I'm sorry, diversity and defense in depth to a specific operating plant.

At the time they did not have a licensee which was going to potentially use the D3 topical report or the MELTAC operating platform.

Also the scope will address diversity with safety and nonsafety systems. The protection and safety monitoring system is a safety and the plant control monitoring system is the nonsafety. Both are using the MELTAC platform.

Inherent in the -- or the premises of the common cause failure affects all common elements to both. And the common element to both the safety and nonsafety is the MELTAC platform. Therefore a common cause failure will disable both safety and nonsafety.

Also we will discuss the functionality of the diverse actuation system. It is analog and nonsafety. It provides a defensive measure to cope with anticipated operational occurrences and also postulated accidents concurrent with the common cause failure. This is beyond design basis.

The task provides the Atlas mitigation function. It also provides automatic actuations where time is insufficient for the manual operator actions.

MHI is proposing -- excuse me -- MHI is proposing that automatic actuation is within 10 minutes from a given event for action required.

Now also there is a delay from the anticipated PSMS trip conditions for the DAS to actuated. And there is also a blocking of the DAS if the PSMS has proper actuation. That is done by feedback from the plant actuated components.

MEMBER STETKAR: Royce, looking ahead I think the answer is yes, but I just want to make sure. Are you going to talk more about the 10-minute operator intervention?

MR. BEACOM: Yes, we are.

MEMBER STETKAR: Okay, I'll wait.

MR. BEACOM: Okay.

The DAS manual actuation, it is done on a separate HSI panel with conventional controls and indicators. And MHI proposing for manual actuation less than 30 minutes from the prompting alarm.

The DAS also receives isolated signals from sensors, which are shared with the PSMS, and the DAS outputs to a discrete portion of the power interface module.

MEMBER BROWN: The 30 minutes, the way you phrased it here, that is for between 10 and 30 minutes --

MR. BEACOM: That is correct.

MEMBER BROWN: Using an alarm for the operator action?

MR. BEACOM: That is correct.

MEMBER BROWN: Which is -- and that is a deviation from ISG-02 right now?

MR. BEACOM: Right, we'll get to that. That is correct.

CHAIRMAN MAYNARD: Royce, could you be careful turning your pages? It's been rubbing across the microphone there.

MR. BEACOM: Okay.

So these five documents are the accepted bases for the implementation requirements of the D3 approach. The first four documents --

MEMBER BROWN: Can you go back a

slide? I just want to -- one of the things that is noted in this as well as in the topical report as well as in the SER is, there was effectively one set of sensors used for everything: protection, ESFAS and DAS. The signals feed straight through, because you have got RPS, and then ESFAS, and then you have the isolation device that feeds over to the DAS.

So effectively if we had no diverse -- I'm being pejorative when I say that slightly -- there is no effective diversity in sensor inputs for any of the three functional protection systems, RPS, DAS or ESFAS.

I'm not saying that is wrong. I'm just saying there is no diversity at all between those -- for all three of the major shutdown protection, ATWS, et cetera, functions.

MR. BEACOM: Yes, one you were using conventional sensors, no software based -- having a possibility for a common cause failure. And two, the concern for a single failure is not an issue due to the redundancy of the sensors.

MEMBER BROWN: Well, if you read the rules, theoretically you are supposed to have diverse sets of sensors; at least that's the way I read them in accordance with the diverse actuating system stuff. Now if that is not exactly right, somebody can fix it. But that is just the way I read it; in other words, if you go through and you read some of the layouts in the SER and in the topical reports, it specifies that. I'm just saying, that is a point that has got to be made, sometime as you draw through this, and there is a number of other commonality areas. For instance the outputs from the DAS are fed back into the PIFs which are used then for actuation functions similar to the RPS and ESFAS.

So there is -- the level of diversity, there is some -- we're commenting stuff up in a little bit more -- to a greater extent than at least what I am used to seeing. I can't speak for what other people have seen in the past, but this is the first time. And it just seems to be -- so that is kind of an issue as it floats around as I'm thinking about what we are doing. So I just wanted to make that clear. You've got it listed, so it's not hidden. But it's kind of an issue.

MR. BEACOM: I don't think -- we haven't run across -- I know a lot of Westinghouse plants. They are diverse sensors used. But that is only for their particular situation. There is no requirement that I know of that requires a diverse sensor to be used.

MR. JACKSON: In fact, the NRC has looked at this for a number of years, and in particular I think about the ATWS rule, 50.62, and basically it said that sensors didn't need to be diverse, even though you needed to provide a diverse means to trip the turbine, initial auxiliary feedwater.

So in that case that ATWS systems use the same sensors and so forth. And we kind of took the pathway, the staff's position is that common cause failure for components is beyond design basis.

So in the past for like the ATWS mitigation systems, we have allowed them to use the same sensors in developing those systems. So that kind of carried on through to the diverse actuation systems also.

But I understand, there is a commonality point there. So if you do have a common cause failure of the analog sensors, you would possibly not be able to accomplish the safety function.

MEMBER BROWN: The whole point of the comment is that there is -- I just don't see any -- there is no way to put a wall at some point between the various three systems. They are all just kind of smushed up together. I'll stop right here and let you go on with the presentation, unless somebody else has --

CHAIRMAN MAYNARD: I made a note of that question. I think we will see how it gets addressed any place else, and it may be something that we want to discuss at the full committee meeting in a little more detail and stuff.

But again it's not whether or not -- well, ultimately it's whether or not it is a problem. I think part of it is getting, what are the requirements.

MEMBER BROWN: Yes, I mean that's what I said. I didn't say it was wrong necessarily; I just -- unsatisfactory at the level of being able to go and look at this. It's block diagrams and a few other things. It's kind of hard to determine that everything is as clean as you would like it to be.

John.

MEMBER STETKAR: I think something you

just said struck a nerve, I think. You said that common cause failures are beyond design basis events. And we are certainly aware of that fact; I'm on board with that certainly.

However common cause software failures seem to be a beyond-design-basis event that we must protect against. And yet common cause sensor failures are a beyond-design-basis event that we apparently fully accept. Is it only -- are we only protecting against common cause software failures because someone decided that common cause software failures are the problem that we should protect against?

MR. JACKSON: We felt that they were basically in the -- and this is kind of communicated in the SECY-93-087, because that issue came up about addressing software common cause failures. And the staff felt that software common cause failures, because of their potential consequences, and the potential that they may be more likely than some other common cause failures, that they needed to be particularly addressed.

So that is why the staff had a certain criteria associated with software common cause failures versus say mechanical or other kind of electrical equipment common cause failures.

And what we anticipate is that for common cause failures that may occur to sensors or other things, that they be handled through other programs such as operating experience, corrective actions programs, Part 21, and so forth.

MEMBER BLEY: Just to toss it in to -- I never thought of it quite in these terms before, but the whole EQ program is really protection against common cause failure of hardware equipment. So it's in the process.

MEMBER SIEBER: For specifics, through environmental influence.

CHAIRMAN MAYNARD: For hardware, if it's a known common cause of course you would fix it. But you have to deal with that. But there are a number of components in there that you are not required to take a common cause failure. You may certainly be able to cope with that, but you have two frames, you have two pumps.

I do think that the software issues are a little bit unique from a regulatory standpoint, even though it's beyond design basis we are going to require that you be able to deal with a common cause failure. So the same requirement doesn't exist for all the components in the plant.

MEMBER ABDEL-KHALIK: I guess the reason I am not overly disturbed by the diversity in sensors is lack of -- or lack of diversity in sensors, if you look at a reactor trip signal, for example, you are getting a reactor trip signal from multiple indications, whether it's steam generated level, or pressurizer. And they are diverse. So you have a common cause failure in steam generator instrumentation. That doesn't mean that you will now get a reactor trip signal from something else that is totally different.

MEMBER BROWN: You can argue, it depends on the analysis. You have to look and see what particular signals are going to trigger a reactor trip. They don't all work in the same way. You put different functions in depending on what particular casualty or accident or postulated occurrence or whatever the terminology, AOOs, et cetera. And that is normally why you have a diverse setup. And if that one fails the other ones may not trip in time to give you that reactor trip; that is the point.

And I don't want to beat that to

death, it's just that -- it's a little counterpoint to your comment, that's all.

MR. SCAROLA: This is Ken Scarola. I'd like to address both of these issues for a moment, the sensor diversity as well as the software common failure if you don't mind.

And the point that you made is a very good one: there is a section within the topical report that speaks to the issue of sensor diversity for different critical functions. And we do make the case, and I know that the staff requested more information on this subject, of sensor diversity for critical function modules.

And we make the case that for every critical function, we do have diverse sensors, even though the sensors are used by all the systems that you identified, they are used by the RPS, the ESFAS, control systems as well as the DAS, diverse actuation system, DAS. There is sensor diversity for all the critical functions.

And you are right, there may be the case where we do credit within Chapter 15 a sensor responding with a specific period of time, and a secondary sensor may respond at a later period of time, but there is in fact sensor diversity there.

That is outside the Chapter 15 analysis. It's essentially a qualitative analysis that identifies for every event we do have multiple ways of actually protecting for that event.

MEMBER SIEBER: But that is not part of the topical report methodology right now. They are not taking credit for it.

MR. SCAROLA: Well, no, it is taking credit for it only to defend that there are two parts of the D3 analysis. One is to defend that the probability of common cause failure is sufficiently low that it can be considered a beyond-design-basis event. So we do make the case of many defensive attributes, including diverse sensors that say, the potential for common cause failure is very very low.

Now in spite of that we accept that there may be a common cause failure, and then we identify how we defend it or what our defensive measures are for that.

But there are two parts of the D4 report. The first is to demonstrate that the potential for common cause failure is very low. And this is one of the reasons why there are these links to the other topical reports, because you have to address the primary protection system.

MEMBER SIEBER: I think that there is diversity in all of these things because there are separate trends. On the other hand, from the standpoint of 63.03, diversity with respect to manufacturer or type of style or what have you, may not be there for Chapter 15 accidents.

And so you have diversity in the classic sense that you used 20 or 30 years ago, but not in today's sense o f 63.03, right? Okay.

CHAIRMAN MAYNARD: Let's go ahead and move on.

MR. BEACOM: We were going to leave the discussion of how the top four documents with their requirements would be met for the closed session later on. MHI did an excellent job of addressing each one of these documents and the criteria within them.

In the findings and the conclusions, for the large break LOCA coping strategy, MHI provided if you will a three-point position. That is the high quality, high reliability measures of the MELTAC electronics platform; the existence of simple application algorithms in its 20 years of existence. Mostly single input and single set points. Provided an excellent basis, also the low frequency of the AAOs, and postulated accident events.

Those represented at an extremely low frequency for common cause failure recurrence. They also work with 2IAEC standards, which suggest a value for probability to figure on demand. Although MHI did recognize that there were no formally accepted methods for establishing software reliability, they did state that they felt that the uncertainty of this was offset by the leak-before-break function.

Now staff found the strategy was unacceptable. They felt that a software latent defect is still a possibility, and that the common cause failure must be considered concurrent with the anticipated operational occurrence or postulated accident.

Leak before break is now authorized in very narrow applications, mostly for the consideration of dynamic effects for pipe ruptures. This is discussed in the NRC inspection manual, Part 9900 on 10 CFR guidance.

Also recently the staff revised the SRP, HICV 19, on guidelines for diversity and defense in depth.

The latest revision is now consistent with a very narrow application of leak-before-break credits.

MEMBER BROWN: The leak before break, this is more trying to learn something here, did they have a leak detection system in here? How is that executed? I didn't see how it's done. I just don't know. Do they have buckets under -- I'm being facetious. How do you do that? Go ahead.

MR. BEACOM: The -- well, there is not a lot of detail. But there is indication on the DAS panel for leak protection.

MEMBER BROWN: I know, but how do you do it?

MR. BEACOM: How do you do it?

MEMBER BROWN: Is it mostly inventory management? I mean water is moving up and down, and pressurized all the time.

MR. JACKSON: In the current operating reactors there is really about four ways. One is, they use a mass balance calculation on the process computer to determine the difference between make up and let down in the reactor cooling system is one way.

Another way is the containment air gaseous in particular, RAD monitors.

Another way is containment structure sumps. And another way is the containment fan coolers.

MEMBER BROWN: All right, go ahead.

MR. JACKSON: I don't know if MHI is actually proposing that in the US-APWR.

MEMBER BROWN: They are going to do it, but they haven't said exactly how they are going to do it?

MR. JACKSON: We didn't get into the technical details of how they would do it primarily because there was a regulatory issue with it, not so much the technical issue with it, but the regulatory aspect. That it was inconsistent with GDC 4. And the application of leak before break in that application. So that is why we didn't find it acceptable.

MEMBER BROWN: Thank you.

MR. BEACOM: Okay also in the findings was protective action, manual versus automatic. MHI had the target of less than 10 minutes for automatic actuation required for given events. And then greater than 10 minutes manual action is assumed. That does different from the digital INC interim staff guidance, where less than 30 minutes is assumed to be automatic. That is not a steadfast requirement but a guideline. The licensee or application can bring to the table what he feels is a sufficient explanation of less than 30 minutes manual action.

However, in the topical report itself, there was insufficient information to assess the manual action between 10 and 30 minutes following the event. This particular justification for manual action will be in the US-APWR HS certification.

MEMBER STETKAR: Royce, now I will ask the question I was going to ask earlier. The staff has just pretty recently issued the new Section 3 to ISG-05, which speaks specifically about the issue of timing of operator actions, and it departs from the hard and fast 30-minute rule, and requires an evaluation of time available for operator response versus time required to complete those actions, within the context of the whole realm of AOOs and Eas, and so forth, to evaluate the design.

How is the staff taking that ISG into consideration as part of this review?

MR. JACKSON: I think like you said there's a recent change to ISG-05, and right now the staff is looking at how to reconcile between ISG-02 and 05, because ISG-02 still has the 30-minute criteria in it.

So we are looking at and discussing among ourselves how to resolve that particular issue. So we will keep you abreast of what is going on between those two ISGs, and --

MEMBER STETKAR: I guess I'm asking within the context, because we are asking -- we are being asked to kind of get feedback from you on the review of this particular topical report, which has the 10 minutes and 30 minute issue --

MR. JACKSON: I will give you my perspective on it. The advantage to the 30-minute criteria gives, especially for new reactor applications, is, we receive an application that basically says we are going to use manual actions, and we are going to use it either post-30 minutes or before 30 minutes.

To use it post 30 minutes the manual actions, we feel comfortable that the applicants can probably demonstrate that, and that would just be basically an ITAAC verification later on. So it's not part of the license review, but if they have sufficient comfort they an do that.

Under 30 minutes, that's where we get challenged, because if you bring in manual actions for, say, five minutes, okay, how much margin is actually there? The staff doesn't really know that to make a safety conclusion at the licensing stage.

Now the applicant may be able to demonstrate it later on when the plant may actually have a simulator and other facilities to demonstrate that. But the challenge is at the review of the design certification stage we don't have that type of information to really base a solid conclusion on, so we're constantly in okay -- the proposal is something that we -- what is the technical basis for accepting it?

CHAIRMAN MAYNARD: We are not being asked to take a position on whether or not the less-than-10 minutes is acceptable.

MEMBER STETKAR: No, no, but I was asking him --

CHAIRMAN MAYNARD: We have had other

discussions about the ISG-05 and stuff. So I don't want to get into a debate on - I think for us, when I look at the SER, they identify specific things that need to be addressed at the application specific stage, either with the DCD review or the COL review.

And I think what we should really be looking at is whether or not we think that those are the right actions, as opposed to the 10 minute versus 30 minutes.

MEMBER ABDEL-KHALIK: When will the emergency operating procedures be developed?

(Comments off the record.)

MR. SCAROLA: The EOPs are actually being worked on now, and they are being developed as part of the DCD phase.

CHAIRMAN MAYNARD: Could you identify yourself?

MR. SCAROLA: Oh, I'm sorry, Ken Scarola, MHI.

CHAIRMAN MAYNARD: I think for me I don't mind throwing this to the DCD review, and get it reviewed there. If it goes much beyond that then I think I start getting more nervous about the ACRS' role and what is going to happen past that.

But if it is going to be addressed at the DCD stage then I think we have a chance to look at that then and see if we think that is reasonable or not.

MEMBER STETKAR: The only reason I brought it up is because this topical report is on essentially -- it gets back to your original question. This topical report is on the design of -- on their diversity and defense in depth design which translates eventually into hardware. And --

CHAIRMAN MAYNARD: And/or manual actions.

MEMBER STETKAR: Well, yes, and part of the hardware design is what is automatic and what is manual. And if all of the decisions on that design are being deferred to the DCD step, it really brings into question what the safety evaluation on the topical report, as a standalone document, really has.

CHAIRMAN MAYNARD: And I do question that. I question the value of a partial topical report SER. But it gets into an efficiency thing, and it is also something that becomes a risk to the designer and the applicant along with some of these things' weight. So --

MEMBER SIEBER: We sort of have this backwards, I think. The DCD comes first. They become the requirements for the OL when you build the plant. So the topical -- if the DCD reference is an approved topical, and the topical says do this and this amount of time, then it is up to the OL applicant to make sure that they do it.

CHAIRMAN MAYNARD: I want to get back to, at this point we are not being asked to make a decision on whether less than 30 minutes is acceptable or not. Our next shot at this is going to be at the DCD review station. And we're making sure of that. And that is the point, if it's not resolved at that point I would start getting nervous about exactly what actions are going to be put in place for a review process decision that is acceptable later.

I don't personally have a problem with -- I would rather see either a clean topical report, SER, that doesn't have any application, or hold off on the SER for the topical report until the DCD review is done. But we are not being asked to make that decision.

I think what we need to focus on on

the manual operator actions is more the things that the staff identifies in the SER that the applicant must demonstrate are those things that are the right things they need to demonstrate

MEMBER STETKAR: The original question I wanted to bring up was because ISG 05 has placed this 30-minute hard and fast fail criterion into more of a state of flux, where it - if you follow it, it requires that the applicant perform evaluations to demonstrate what the appropriate break between automatic and manual action with some justification.

And I recognize the timing of the reviews and submittals, and bringing this to the ISGs, is difficult. The question initially was, how is the staff considering that. And I guess the answer is, not necessarily within the context of the SER or this particular topical report, but probably within the context of the final DCD.

MR. SCAROLA: Excuse me, this is Ken Scarola, I'd like to make a comment that I think it's important that we understand the timing here. This topical report was submitted to the staff in March of 2007. At that point in time there was no ISG-02, so there was no 30-minute criteria. There was no ISG-05, so there was no criteria for demonstrating the acceptability of any manual actions.

So the intent of this topical report was to propose to the staff our methodology for demonstrating the acceptability of manual operator actions.

We did not draw a 30-minute line. We said that any manual actions we would demonstrate their acceptability by a thermal hydraulic time availability analysis and an HFE analysis to demonstrate that the operators could take the actions.

Those thoughts that were documented in this topical report were the basis for ISG-05, which ultimately got documented.

So I think you need to understand where we had this timing issue, and hopefully we can bring this all to closure.

MR. BEACOM: Let me also add, since we are doing pretty good in time, due to the nature of the D-3, there is a lot of tentacles, a lot of information that goes out, away from INC, that we have to bring in. This is also almost a first time attempt at a topical report applying a

D-3 approach.

Usually it is within the licensing itself for a particular plant. As you also see other INC topical reports and the resulting SERS, there is a lot of application-specific items that have to be answered before you apply a particular platform to it. That would be the existing SERs for digital INC platforms such as Triconics, Teleperm, and the Common Q lines. Those have at least the 10 -- or 16 I think it is different application specific items that have to be answered before you apply that platform.

So I think due to the nature of these three, and that is even beyond information leaks normally provided in an electronic platform SER. We need a lot of information coming from operators disciplined in the activity. So we will get back on track here.

So in the findings and conclusions, the staff concluded that the D-3 approach in the analysis provided that was done per NUREG-6303 had met the acceptable basis for conforming to the requirements and supporting industry standards.

This was all subject to the satisfactory completion of the application-specific action items.

And we go on to look at each of the application-specific action items. As you can see the need for each one, there are a lot of factors involved with it. I will try to bring them up as we go through each one.

The first one, or the isolation devices, this is being reviewed in the MELTAC's offices. This is necessary in order to confirm that we have a path from the sensor to the actuating device that is a non-software based, not susceptible to a common cause failure.

The second one is what we were just discussion: manual actions. Also the concept in the application for specific implementations of priority alarms. That has to be demonstrated. That is part of the HSI effort.

Another item that is going to be part of the MELTAC topical report review is for the PIF module and its susceptibility to common cause failure. That like the isolation module is critical.

MEMBER BROWN: They made the statement in their topical report that it is not.

MR. BEACOM: They did?

MEMBER BROWN: In section seven or something, it is not. And if there is no software in it --

MR. BEACOM: We'll trust that, but we will also verify.

MEMBER BROWN: But it specifically talks not common cause failures, generically; it says software common cause failures. Which is fine. So if they have no microprocessors in it, then that one seems to have -- I walked down that one fairly easily. But I don't know what's in it.

MEMBER STETKAR: I am assuming we will find that out.

MEMBER BROWN: I am hoping. I'm just noting that they made the flat statement, and hopefully that will be --

MR. JACKSON: Actually in the proprietary session we can talk a little bit about the design. We have seen the actual board in Japan, based on the MELTAC report.

MEMBER BROWN: Okay, all right, let's go on. Because I've got some other questions I don't know whether they were suitable for closed versus open.

CHAIRMAN MAYNARD: If you don't know

it doesn't hurt to ask. I think that the staff and MHI need to tell us if we are getting into.

MEMBER BROWN: Okay, then when you finish this, before we leave, I've got a few other -- couple of questions I wanted to at least get on the table so that we can make sure that people think about before we get into a later session.

MR. SCAROLA: Excuse me, Ken Scarola, just a point lf clarification. IN the report we do address both hardware common cause failure with the PIF module as well as software common cause failure for the PIF; both are addressed.

MEMBER BROWN: Then I missed that.

MR. SCAROLA: Because for the ATWS rule --

MEMBER BROWN: I looked at paragraph 9.4 is where it said the PIF module are not susceptible to a software common cause failure, because they are consistent, prudent, simple and fully testable hardware devices. I thought it was a fairly clean statement to me. That's why I said --

MR. SCAROLA: But the PIF is susceptible to hardware common cause failure.

MEMBER BROWN: I agree with that.

MR. SCAROLA: And that is why we don't use if for the ATWS rule complaints. And that -- we tried to make that point very clear, because the ATWS rule, we have to address all common cause failures except sensors.

CHAIRMAN MAYNARD: Okay.

MR. BEACOM: ASA number four has to do with the DHB, the diverse HSI panel and its specific controls and indications on it. The topical report has a generic set. The coping analysis has further definitions. But we also identify it specifically for the US-APWR.

ASA No. 5 deals with the final determination of the setpoints and the response time for the DAS. ASAI six deals with the demonstration of the QA process for the entire DAS system meeting the guidelines of generic letter 8506. Essentially the ATWS quality requirement.

Now number seven, number seven you may recognize as the specific acceptance criteria to BTP 19, the guidelines for diversity and defense in depth. This should be addressed by the coping analysis. That Is a technical report as an attachment to the US-APWR.

Also ASAI No. 8 is also an acceptance

criteria for BTP 19. And that also should be addressed by the coping analysis in US-APWR design certification.

MEMBER BROWN: is that BTP 7-19?

MR. BEACOM: Seven dash 19.

MEMBER BROWN: Okay, we keep leading off the seven, and I anted to make sure there weren't multiple 19s out there somewhere.

MR. BEACOM: When you are in chapter seven --

MEMBER BROWN: That's fine.

MR. BEACOM: Number nine is, the applicant should address the partial failures of the PCMS/PSMS, and demonstrate the adequacy of the D3 strategy.

In ISD staff guidance 02, the staff position was that the simple fare -- the total system may not be the worst case, particularly in analyzing the time required for identifying responding to the conditions. It is a common cause failure condition.

For example, a failure to trip may not be as limiting as a partial actuation of the ACCS with indication of a successful actuation.

In other words, we have addressed

common cause failure internal within the topical report in the SER. We also believe that has to be -- partial failure has to be addressed also.

MEMBER STETKAR: Kind of related to that, I had a question. The -- how to put it? -- the analyses that I have seen that I read about talk about looking at common cause failures within PCMS/PSMS, and their effects. Does DAS mitigate those common cause failures?

There was also an analysis that looked at failures within DAS I think within the topical report. And can that affect PCMS/PSMS.

There is this kind of a third and sort of subtle, are there any failures within PCMS or PSMS that can also cause failures of DAS? And I'll bring this up in the closed session probably because it gets into a little bit of the details. But would that fall -- the reason I'm asking now, would that fall under this general application specific action item number nine? Are you asking -- you specifically mention partial failures, but I was curious whether you are looking at only a subset of a particular set of failures, or whether that is more of a broad brush look at practical failures among PCMS, PSMS and DAS, whether they are categorized as partial or whatever name you want to have on them.

MR. BEACOM: Well, I did identify what we thought was a partial failure which was a subset of common cause failure.

MR. JACKSON: I think this is kind of like the discussion we had about the common sensors and the PIF modules and the staff did review what were the common parts where you could have potential failure that affect both systems. I think the thing Royce was talking about here, with partial failures, is the PCMS or PSMS may partially actuate. So it may appear to operators that the system is fully actuated, but in fact it is only partially actuated.

So that kind of brings in some elements possibly of human factors, evaluation and stuff. So that is why left is as application specific action.

MR. BEACOM: But you are going to tell us your concerns later.

MEMBER STETKAR: It is partly, it gets into some details of the design in a proprietary sense.

MR. BEACOM: And then item 10, the

applicant shall provide an acceptable defense and depth in diversity strategy for the large break LOCA, current with the common cause failure of the PSMS not including the LBB.

And then 11 is within the topical report itself where it identifies in Section 10 future licensing submittals. Those have to be all submitted and satisfactorily completed.

So that is all I had for the non-proprietary version.

MR. BEACOM: Okay, anybody got any questions?

MEMBER BROWN: Some of mine deal with details, also, so it might be -- you want me to go ahead and at least voice them?

CHAIRMAN MAYNARD: Why don't you just go ahead and voice the question. Then if they look like -- we can delay it until then so we don't get behind schedule. That's fine.

But one of the thing I noticed in going through there, the first one is the top level it requires both DAS subsystems to operate in order to initiate an automatic action. There is two sets.

The second is, the DAS is blocked

manually during startup and shut down, which I didn't -- I need to think through that. I think it bears some discussion about why you do that, what the thought process is.

And the third is the DAS is also blocked by the normal reactor protection system. If it trips, and then there is -- in spite of the 10-minute delay for its reaction, there is another block.

MEMBER STETKAR: It's not a block, though. I looked at that.

MEMBER BROWN: I just wanted to get it on the table. It is mentioned on -- excuse me -- page 30, figure 623 -- figure 6.2-3, it shows a little block diagram, and has some ands and ors and all that kind of stuff. And so I mean, that is the way it looked as if it had blocked. And if we can have some elucidation on that, that would be -- so there are three areas here. The system is supposed to be there as a backup, and we've got three circumstances -- well, two circumstances where we are being blocked basis on specific signals or operation; at least it appears to. And one case where you require both to operate.

I can understand that, because you

don't want one to fail and inadvertently initiate something, but that -- here is the diverse actuation system, it's got some rubbery requirements floating around in it, that's all.

CHAIRMAN MAYNARD: And that is probably enough said. Because if we go into too many details on the question we might actually start getting into proprietary information.

MEMBER BROWN: All right, so I just lay that one on the table.

MEMBER ABDEL-KHALIK: I have a question about item number two, which relates to the application-specific implementation of the priority alarms should be adequately demonstrated.

That just seems to be something that can be demonstrated, adequately demonstrated way way late in the process.

MR. JACKSON: Basically the item #2 there addresses the human factors analysis portion, so what HMI has proposed is to use something called a priority alarm, which are basically -- be connected to the DAS and say, there is a common cause failure, alert the operators, prompt them that there is a common cause failure.

For INC aspects, we don't really have an issue with putting the alarm onto DAS, but from a human factors evaluation standpoint, they would need to evaluate and say, and determine that the use of that kind of alarm, is that acceptable to meet the manual action time requirements.

MEMBER ABDEL-KHALIK: Your definition of this is probably a lot narrower than my interpretation of what this requires. What did you understand as to when you will be able to adequately demonstrate that this application specific implementation of the priority alarms would take place?

MR. SCAROLA: There are really two phases to this, Ken's rule, MHI. It was our intent through this topical report to demonstrate the basic technique of how we generate the alarm, which is independent of the PSMS, and how the PSMS blocks the alarm if the PSMS functions correctly. That was something we thought we could demonstrate generically. The staff has left that as an application specific item.

But the final demonstration of any specific alarm is done through the HFE analysis that is done in conjunction with the coping analysis. So for the coping analysis we do two things: we demonstrate first what th e required action time is based on the thermal hydraulic analysis, and then we identify the specific alarms, when the alarms come in, and then the EOP steps that the operator must executed to get to the credited manual action.

So the event is time zero. The alarm is sometime later. And then the operator action is sometime later.

That can be demonstrated two ways: first analytically, but then ultimately we validate that in our full scope simulator.

So the final validation, you are right, is very late in the process. But the analytical demonstration, we have been doing that now; that is part of the DC data.

CHAIRMAN MAYNARD: The bottom line is it's going to have to be demonstrated before a plant is allowed to operate, and the further it goes into the system, the more of a risk somebody is taking that they may have to go back and do a design change.

I don't know if it's going to be able to be done at the DCD stage or not. It could very well end up being another action item for the COL to demonstrate.

I think at the DCD stage is where I would want to go into it in a lot more detail as to are the controls really there if it goes to the next stage.

MR. SCAROLA: Well, this phasing is addressed in ISG-05. ISG-05 recognizes that you can demonstrate this analytically during the certification phase. But it also identifies the need for an ITAAC for final validation through full scope simulation, and that of course will occur later.

CHAIRMAN MAYNARD: Okay. Any other questions? If not, let's take a 15-minute break. Let's be back at 10 after.

(Whereupon at 9:53 a.m. the proceedings in the above-entitled matter went off the record to return on the record at 10:09 a.m.)

CHAIRMAN MAYNARD: Okay, let's start up again here. So let's come back into session. And this session is open session on the Class 180 gas turbine generator system, and is it Mr. Niida? Or Mr. Kawanago.

MR. KAWANAGO: We have to be introduced by ourselves. And my name is Shinji Kawanago. I am licensing manager of DCD and also the COLA of MHI.

And also that today's presenter is also the same first name, Shinji. I realized it's complicated.

MR. NIIDA: My name is Shinji Niida. I'm an electrical engineer of MHI. And also --

MR. SPRENGEL: Ryan Sprengel, DC licensing for MHS.

MR. KAWANAGO: Today we would like to explain by using this opportunity on what is a gas turbine generator, and also we would like to explain the reason why MHI has selected gas turbine generator as an emergency part of our system. And also we would like to explain why MHI can select the gas turbine generator. And also that we know it is one topic, and it's the reliability of the gas turbine generator, and we would like to explain the reliability of the gas turbine generator, and also we would like to explain the content of the test PROM, and also the binary, the diversity of the -- between the emergency parts of our system and alternate safety process.

And today we prepare this presentation, but only the non-proprietary portions. And we would like to explain, and by using this non-proprietary version. And if we have questions from you, and when e have questions from you, and if we need to explain to you by using proprietary information, in that case we will answer in accord.

And also, if you have questions at any time, it's okay to ask it, okay.

CHAIRMAN MAYNARD: I would like to remind the members here that this is an informational -- and that we will try to keep things moving along. I think it's good to understand this. I think it's good to get into some of the data and everything. But I want to make sure that we leave time for the main purpose, so go ahead.

MR. SPRENGEL: To clarify real quick, we don't have a separate -- there is not a separate proprietary presentation. So this is it, if we have further questions. So this will be the whole presentation.

CHAIRMAN MAYNARD: And I think,

correct me if I'm wrong, I think that probably one of the things we want to make sure we spend some time on is on the data supporting the reliability of these units. I think it's good to have an overall understanding, but our focus ends to be on the data used to demonstrate reliability.

MR. KAWANAGO: Okay, this presentation consists of two portions. First, I'll explain about AAC GTG, that specification or advantage or disadvantage of GTG. And reliability, et cetera. And next I explain about non safety related AAC-GTG specification, where operation under poor conditions and the diversity, et cetera.

First, introduction. The US-APWR uses Gas Turbine Generators as Emergency Power Supply in lieu of the commonly used diesel generators.

The reasons why we selected the gas turbine, one is the gas turbine is very simple rotating engine with few components. And the gas turbine generator system consists only of the gas turbine engine and generator, and the fuel transporter, starting and control instrumentation systems.

And water cooling system is not

required. And --

MEMBER STETKAR: Mr. Nida, I thought I read somewhere, this particular gas turbine is actually two parallel gas turbines. Your gas turbine unit is actually two --

(Simultaneous speakers.)

MEMBER STETKAR: -- in parallel. It's not a single machine like a diesel generator?

MR. NIIDA: Yes.

MEMBER STETKAR: Okay, I just wanted to make sure. I thought I had read that, and I wanted to be sure that we understood that correctly.

MEMBER BROWN: Okay, I thought I gathered that also, but I guess the question didn't hit me the same way. Two gas turbines, two generators --

(Simultaneous speakers.)

MEMBER STETKAR: So it is a little more complicated than a single driving engine directly driving a generator?

MEMBER SIEBER: Yes, but it's no reciprocating parts.

MEMBER STETKAR: Okay, continue, I just wanted to make sure that I understood.

CHAIRMAN MAYNARD: Charlie, you had a question.

MEMBER BROWN: The sharing, I guess, the size of the turbines, the gas turbines, excuse me, is either one of them suitable for supplying the full -- you need both in parallel for the electrical capacity fo the generators?

Are you all shaking your head up and down? In other words I need both gas turbines operating to be able to take the full electrical capacity of the generator?

MR. KAWANAGO: Our design is a full twin system. And so we have four systems of gas turbine generators, so thats 50 person times four. So one gas turbine engine and turbine diesel twin -- it's a twin engine -- counts power supply as 50 person.

MEMBER BROWN: Okay, I got that.

MEMBER BLEY: I don't know if I read this or not. If one of the two turbines fails, can the other one still drive the generator at lower power?

MEMBER SIEBER: It depends on how it fails.

MEMBER BLEY: That is kind of what I

was getting at.

CHAIRMAN MAYNARD: Let's move on. I think that is something we would be interested in when we got to a DCD stage with this type of configuration as to what happens if one fails and one doesn't. I don't think we have to address that now. But I do think that would be something important to note.

MEMBER BLEY: Eventually we will want to know.

CHAIRMAN MAYNARD: Yes, we will.

MR. SCAROLA: Ken Scarola. I think it's important, though, to understand that we are not taking credit for any redundancy of those engines within a single division. There are four separate divisions, four separate GTG pairs.

MEMBER STETKAR: We are just talking about the thing inside a pack, what you are calling the gas turbine generator package.

CHAIRMAN MAYNARD: Okay, let's go ahead.

MR. NIIDA: And the last reason the GTG presents a high level reliability. In the case of the application of gas turbine generator system for nuclear power generation should reconsider the high reliability and the capability. To meet this requirement the combination of an extremely reliable aircraft component with equally reliable industrial components such as the reduction gears, electrical generator, governor, voltage regulator, relays, and similar component is selected. The advance accumulator design of US APWR allows a starting time for the gas turbine generator of under 100 seconds.

And this slide shows advantages and disadvantages of gas turbine generator. First off gas turbine generator system is very compact, smaller than DG, and cooling water is not required. Very simple system. Periodic maintenance of gas turbine generator is require, less than diesel generator. And reliability, gas turbine generator is expected to be better than the DG. But the starting time, the starting time of gas turbine generator is longer than DG, about 40 seconds.

And noise level, high frequency levels are ease to silence. And the vibration: very small levels because the engine is not reciprocating.

MEMBER BLEY: I am sorry, I didn't

hear the last sentence.

MR. NIIDA: Gas turbine is not reciprocating.

MEMBER BLEY: Oh, okay.

MEMBER STETKAR: You mentioned cooling water is not required. You mean external cooling water? It has an internal cooling --

MR. NIIDA: Gas turbine can be cooled by surface air ventilation.

MEMBER STETKAR: But do the gas turbines themselves have their own internal cooling water loop?

MR. NIIDA:

MR. KAWANAGO: Basically, the gas turbine generator is completely the same as the design of jet engine.

MEMBER STETKAR: Okay, thanks.

MR. NIIDA: And frequency variation is very small rather than DG. And exhaust gases: low levels since combustion efficient is high.

This shows, this is one line diagram of US APWR gas turbine system. Blue lines show Class 1E safety related buses, and red lines shows non Class 1E, non safety related onsite AC buses.

And there are four class 1E medium

boldface buses, and each gas turbine generator is connected to each bus.

And this slide shows design specifications of Class 1E GTG. First, Class 1E GTG Class 1E, Seismic category one, and there are four 50 percent units. And rated capacity is 4,500 kilowatt continuous condition. And 4,950 kilowatt short time capability.

And rated voltage is 6.9 kV.

MEMBER BLEY: It is not of great importance, but I noticed some of the specifications of this list are different from the ones I saw in the test plan. This is the actual data for the US APWR gas turbine?

MR. NIIDA: Yes.

MEMBER BROWN: This is for one gas turbine generator unit?

MR. NIIDA: Yes.

MR. KAWANAGO: One gas turbine generator unit.

MEMBER BROWN: Before you go on, on the previous page, I lost the bubble here for a minute, where is the gas turbine in here? At the bottom?

CHAIRMAN MAYNARD: At the bottom.

MEMBER BROWN: Oh, my glasses don't work well enough on the small print. Okay, so the blues are the Class 1E, and the reds are the regular AC -- okay, got it, thank you.

MR. NIIDA: This Class 1E GTG's air starting time. Air receivers of each train have capability to start the GTG for three times. This GTG uses diesel oil and the fuel storage tank of each train has capability to operate GTG during seven days on continuous rated capacity.

And fuel tank of each train has capability to operate GTG during 1.5 hours under continuous rated capacity. This is similar to nuclear energy -- diesel generated.

And Class 1E GTG should satisfy with requirements of voltage and frequency variation in Reg Guide 1.9.

This shows the engine itself. And this shows a typical GTG --

MEMBER BROWN: Before you go on, the last picture, this is -- which part is the -- I guess I can tell which part the turbine motor is. But obviously you didn't just take a jet engine off of a 787. So there are other pieces that go with this, that are non-aircraft proved --

MEMBER SIEBER: The whole thing is really non-aircraft.

MEMBER BROWN: Well, I'm just using the words that he used earlier, were that we took an aircraft engine --

CHAIRMAN MAYNARD: This is very similar to smaller aircraft engines, not your big commercial airliners. It's more like the smaller, because this uses centrifugal compressors rather than axial flow compressors. The main difference, something like this, than a small one is, a small jet engine is going to have fewer turbine stages. This uses a turbine purely to drive a mechanical device, rather than having any thrust.

MEMBER BROWN: No, I understand. I'm just looking at the input -- there just seems to me -- there are some differences, so it's not like you just transplanted something over. It's got to have a qualification program of some kind to make sure you've got all the other parts connected and working right.

I didn't work much with gas turbines; that's why I'm asking.

MEMBER ABDEL-KHALIK: There are two compressor impellers here. Is there an intercooler?

MEMBER SIEBER: Not on these. But typically on big gas turbines there is.

MR. KAWANAGO: We need to check, and we will find out.

MEMBER ABDEL-KHALIK: Right, because that relates to the previous question whether this is totally air cooled.

MR. KAWANAGO: Right, the air cooling. But regarding intercoolers, we will check and the answer later.

MEMBER BROWN: Well, you say that, Said, to go back to slide #12, the cooling system, water cooling, preheat, is needed for quick start.

(Simultaneous speakers.)

MR. SPRENGEL: The columns.

MEMBER BROWN: Thank you. I thought we were just walking -- I apologize.

(Off the record comments.)

CHAIRMAN MAYNARD: I think we are ready.

MEMBER BLEY: Maybe your associate could use the mouse to point?

MR. NIIDA: This is a gas turbine package, engine, generator, this turbine, this enclosure. And this is a control panel and a battery panel. And this is a fuel tank. And this is a ventilation intake duct. And number seven is a ventilation exhaust duct, and number four is exhaust silencer.

This is a typical system.

MR. KAWANAGO: And this one, as Niida-san said, on a typical gas turbine package. And in the industry when we apply this gas turbine generator, basically on a starting system, is a DC motor. So this system has a battery pack. But our application for the nuclear power plant we use the air starting system, not the DC motor.

MEMBER STETKAR: Just for clarification. For the safety-related gas turbines you are going to use air start. For the non-safety gas turbines, will they be air start, or will they be DC?

MR. KAWANAGO: DC.

MEMBER STETKAR: Okay. Those will be DC. Thank you.

MEMBER SIEBER: Which is the prime source of failure.

MR. NIIDA: The next slide shows the inside of an enclosure. In the enclosure these are two engines. This is two engines, and this is gear box, reduction gear. And this is generator. And this is starter motor.

This figure is DC starter motor. But we use the air starter motor.

CHAIRMAN MAYNARD: Is your air starting motor, is it like the DC motor only it is air driven?

MR. KAWANAGO: Yes.

MEMBER ABDEL-KHALIK: Is this going to be a separate air compressor than the air system you have for the plant?

MR. KAWANAGO: Basically those designs are almost the same as typical diesel generator. So we have the separate air system and those are the compressors.

MEMBER ABDEL-KHALIK: Okay.

MR. NIIDA: On the GT air inlet if you used both combustion vent air outlets. This is battery outlet, and it goes out through this exhaust silencer.

The next slide shows supporting system for gas turbine. First fuel system. Fuel system of gas turbine is almost serial to the EDGs. Fuel system is designed based on requirement for safety-related EDG system. Next lubricant oil system. Amount of consumption of lubricant oils is less on DGs. And the system is simpler than DGs, and the system components are fewer than DGs. The lubricant system is used for both engine and generator. Also preheat of lubricant oil is not needed. And starting system, starting air system of the GTG is almost similar to the GS before we explained. Air rotors rotate at the DG. And starting system is designed based on requirement for safety-related EDG system.

Cooling system, water cooling is not needed. Self ventilation fan can cool in the generator package. And next inlet exhaust air system. Inlet exhaust air system consists of that fan and exhaust. Inlet air is used for both combustion and ventilation. Vented air is discharged and exhaust is discharged via the exhaust silencer.

I&C governor and AVR control is similar to DGs. Monitoring parameters and protection signals are different from DGs. Control logic of the GTG is designed special to GTG, and logic is installed in Class 1E control cabinet.

And the next: auxiliary power.

Auxiliary power is designed almost similar to DGs. The pumps, fans are supplied power from the Class 1E ac 480 volt plant power system.

And starting air valves, excitation of the generator, and control circuits are supplied power from Class 1E dc 125 volt plant power system.

For next slide I explain control and protection of GTG. First I explain startup. Starting logic is designed to satisfy with requirements of safety related EDG system. The Class 1E GTGs are started by the following methods. One is automatic starting by the ECCS signal. And automatic starting by an undervoltage signal and degraded voltage signal on the Class 1E MV bus to which Class 1E GTG is connected. And manual starting from main control room, and manual starting from the GTG room, and manual starting from the remote shutdown room. Next.

Starting time. Starting time with GTGs is required within 100 seconds by safety design and analysis for US-APWR. For GTG to reach this voltage and frequency, a GTG breaker should be closed within 100 seconds after starting signal is initiated.

Our GPS 6000 can reach said voltage and frequency within 40 seconds as the standard specification.

MEMBER BROWN: So you are just taking advantage of whatever its characteristic is? You didn't have to do anything to achieve this other than starting? And your analysis gives you about twice the amount of margin.

MEMBER BLEY: As you go to this next one, is this after you have already come up to voltage and frequency? When does the time zero start on this chart? The one you've got on there now. Are you loading it before it's up to speed and voltage?

CHAIRMAN MAYNARD: From what I understand, I think zero starts at the end --

(Simultaneous speakers.)

MEMBER BLEY: They have 100 seconds to get everything up. When do they really start?

CHAIRMAN MAYNARD: Well, let's let them answer the question. I think I know the answer, but go ahead.

MR. KAWANAGO: We are so sorry. This one is -- there is a typo. And the meaning is one -- ten is the meaning, 100, 100 seconds. And of course as we explained to you, this gas turbine generator start within 14 seconds. But in that safety analysis we used 100 seconds.

And so from the 100 second and breaker using 100 seconds, and gas turbine unit, and these are rated for speed, and also rated on voltage. And --

MEMBER BROWN: We got it. So the point being, just to make sure it registers in my brain, the 100 second point is when the breakers close on the TG, on the gas TG, and now you can start sequencing the load? So the 100 seconds is the starting point So everything out from there is 100, 200, 300 seconds?

CHAIRMAN MAYNARD: I don't think that's right. Maybe look at your chart and your labeling on the bottom there. I think -- that still doesn't work there. I think this is the sequencing after it starts there. But those -- that's not 100, 200, 300.

MR. SPRENGEL: No. I think time zero is after we're at power voltage.

MEMBER BROWN: Time zero is really that ten point.

CHAIRMAN MAYNARD: I believe what

that's doing is that the zero time is the time that the gas turbine gets up to speed. There is probably a 10-second stabilization, and it's a sequencing, it probably starts on every five to 10 seconds.

MEMBER BLEY: And it could be when the output breaker starts.

MEMBER BROWN: But it's supposed to be shut by 100 seconds, the output breaker is shut, according to the previous slide.

CHAIRMAN MAYNARD: That will become important to us when we're doing that. But the scale on that bottom needs to be looked at. Go ahead.

MR. NIIDA: On this slide shows the protection sequence. The following trip protective functions are provided during the operation of the Class 1E GTG. One is overspeed, and generator differential current, and a high exhaust gas temperature, and failed to start, overcurrent, and the low pressure lube oil, and high pressure lube oil, and anti-motoring. These are a little bit different. But during operations of the Class 1E GTG under a LOCA condition all protective functions are bypassed except for overspeed, generator differential current, and high exhaust gas temperature.

MEMBER SIEBER: By the way I think that the previous slide is so important that we ought to really understand what's going on, particularly in the zero to 10 step. Right now it's not clear to me.

MR. SPRENGEL: We may be able to come back to that later.

CHAIRMAN MAYNARD: Probably the output breaker is closed.

(Simultaneous speakers.)

MEMBER BROWN: The previous slide said breaker closed by 100 seconds. That's all I'm saying. They said that very specifically.

MR. SPRENGEL: I understand the confusion.

MR. NIIDA: On this slide I explain the whole GTG system, the features of this GPS turbine. No cooling water is required, and it is easy to reduce noise level, and less vibration in high seismic registers, high reliability of the study, and less maintenance, high stability of the voltage frequency, and compact installation, and clean emission. There are many advantages.

And next slide shows --

MEMBER BROWN: Can you hold on a minute? Question for you all on the other diesel systems. And I'm just relating back to my experience in the Navy. We placed very few protection functions on the emergency diesels for applications to safeguard systems. For instance, overcurrent, I didn't put an overcurrent trip in to my diesels. I did not put differential currents in and stuff like that, just because we wanted the system -- we wanted to trip the diesel off because we wanted the system to do whatever it could. Now is there a different --

CHAIRMAN MAYNARD: We did have a number of protective trips. I don't know that there were this many. But where you had two of them, you tried to protect the things -- you didn't want it to totally destroy it. But you might be able to fix and recover that diesel. So the number of trips went way down, and there probably were only three or four, something like that.

MEMBER STETKAR: This is a pretty standard --

(Simultaneous speakers.)

MEMBER STETKAR: And all the ones they have tracked are also pretty standard for normal diesel engine when it's started in a non-safety start.

MEMBER BROWN: I agree with that, that's fine. But on a safety start you still run stuff like the differential currents and --

(Simultaneous speakers.)

MEMBER STETKAR: They have some generator protection. It could be a reverse power; it could be differential current. There is usually one generator protection. One basic mechanical protection like the engine overspeed.

(Off the record comments.)

CHAIRMAN MAYNARD: Or also it doing damage to something else.

MR. GILL: If I may clarify, this is no different than the current position on diesel generators. It is the same philosophy, the same logic. The only difference here is that they have the high exhaust trip which is added; diesels don't have that.

MEMBER BROWN: I am happy --

(Simultaneous speakers.)

MR. KAWANAGO: But I would like to

emphasize one thing. Typically, these are the parameters, it's related to the cooling water. Cooling water pressure and also cooling water temperature, regarding the temperature it's high, and the diesel generator needs additional.

MEMBER STETKAR: But they typically don't have high lube oil pressure, so the tradeoff --

CHAIRMAN MAYNARD: Let's go on.

MR. KAWANAGO: This table shows standard specifications, our M1-T33 gasoline engine. This is continued, I will skip.

And the next slide shows --

MEMBER ABDEL-KHALIK: Can you go back to the previous slide. I think the slide I have numbered is 19, the allowable temperature range is 41 to 104 degrees F? There are a lot of places where the temperature goes way below 41.

CHAIRMAN MAYNARD: Is that the temperature in the room?

MEMBER ABDEL-KHALIK: The temperature in the room, rather than --

MEMBER BLEY: I am assuming that. That's usually -- you mean the incoming air temperature? That is not the incoming air temperature?

MEMBER SIEBER: No.

MEMBER BLEY: Or we're in trouble.

MEMBER ABDEL-KHALIK: Let's find out what they say. Is this the incoming air temperature?

MR. KAWANAGO: We would like to explain regarding this range of temperature . And this is typical, recommendations from Kawasaki, who is the supplier of the diesel powered generator. And so this is -- this value range is actually the typical specification for the other catalogue. And in the application for the nuclear power plant we changed this.

CHAIRMAN MAYNARD: Okay, but is that the intake air temperature or is that the room temperature? What temperature are you talking about?

MR. KAWANAGO: Intake.

MEMBER BLEY: It is intake?

(Simultaneous speakers.)

MEMBER ABDEL-KHALIK: So what is the answer? I'm sorry. This is the intake air temperature?

MR. KAWANAGO: Intake.

MEMBER ABDEL-KHALIK: And you said something about you changed this spec?

MR. KAWANAGO: Especially this, on the higher side, one to four, four applied to the nuclear power plant. Go back to page eight and you can see, the one, two, three, four --

MEMBER ABDEL-KHALIK: One fifteen. But I'm more concerned about the lower limit

MR. KAWANAGO: Lower limit, actually we don't care. Because--

MR. GILL: If I may interject, the staff asked this very question in RAI, and the response we were given, the system has a pre-heat system. So the cooler air is preheated before it gets to the gas turbine.

They can clarify it, but that is the response we have from MHI.

CHAIRMAN MAYNARD: Okay. We can go ahead and move on. I think this is something, when we do our DCD review of the diesel we are going to be interested in this temperature range, and how that is actually --

MEMBER SIEBER: That's not totally satisfactory. Because the preheat system is usually exhaust air heating the intake air, and before you ignite the combustion or fire off the combustion chamber, you don't have any heat coming in there. What is important as far as intake air is concerned is temperature and vaporization of the fuel in the combustion chamber, and at what temperature will that fuel ignite. And that determines when time zero is for start.

So you really need to know the air intake temperature at the instant the starting sequence takes place.

CHAIRMAN MAYNARD: Again, I'd like to move on, because it's not important that we resolve this in this discussion. I think it's fair to say that when we get into our review of this we are going to be interested in that temperature limit, what it's for, and how you manage to stay within that envelope there. So let's go ahead and move on.

MR. NIIDA: This slide shows the size of gasoline packages. The gasoline is very compact compared with diesel generator.

Next slide, this slide shows details of air starting system. This is similar to DG system. Air system consists of an air compressor, and an air tank, and a starting valve unit.

From this slide --

CHAIRMAN MAYNARD: I'm sorry, I want to make sure on that, now you have two turbines in a unit there. Now do you have -- does one air tank supply air to both of those units? Or do you have two air tanks?

MR. KAWANAGO: I just want to make sure.

MEMBER BLEY: While they are looking slide 11 is a little more --

MR. KAWANAGO: We will check that, and we will answer later.

CHAIRMAN MAYNARD: Okay, go ahead.

MR. NIIDA: On this slide I want to explain about evaluation, important input from it and data to safety analysis and PRA in four ways. One is starting time should be within 100 seconds, and fuel storage tank should have seven days kept steep, reliably the target is the same as U.S. nuclear EDGs. For Fail To Start, mean value is four time ten to the minus three power of demand and then 95 percentile is 1.5 times 10 minus two power of demand, and for Fail To Run mean value is 8.0 time 10 to minus fourth per hour, and 95 percentile is 2.0 times 10 to minus three per hour.

MEMBER STETKAR: Mr. Niida, before we start talking about a lot of very small numbers, I'd like to understand what your definition of a gas turbine generator is, and what your definition of a diesel generator is, because that is very very important for me to understand how you are calculating these very small numbers and what they mean.

So for example if I look in a figure, 1.1-1, in the gas turbine qualification test plan, there is a little dotted line that defines what is the thing that you are calling a gas turbine generator. If I look at NUREG_CR/6928, which you refer to for diesel generator data, there is a specific definition of what is included in a diesel generator.

Now I will point out that in the diesel generator data are included the diesel engine with all the components, the electrical generator, the generator exciter, the output breaker, the combustion air supply, lube oil systems, fuel oil systems, starting compressed air system, local instrumentation and control circuitry, and for systems that are cooled by service water the last valve to supply cooling water.

Your block diagram excludes from the gas turbine any remote control and surveillance signals, so any signal that comes in to start the system. It excludes the starting air system. It excludes the fuel supply. It excludes any engine and generator cooling. And it excludes the generator output breaker.

So it seems that your numbers for a gas turbine are combined comparing the reliability of a set of equipment that you define to the reliability of a different functional set of equipment; in fact a larger set of equipment that is reported in terms of diesel generator reliability.

Do you have any comments on that? Because it is difficult for me to understand how to compare two very small numbers when they are actually applying to different sets of equipment.

MR. KAWANAGO: Basically at first, and we need to understand, regarding a diesel generator, we have already had application to the new nuclear power plant. So and to define the actual scope of the, the finished scope of the diesel generator. And we can easily define, and also the third scope, should be identical to the unit on the other side and so on. But on the other hand, and regarding the discussion of the generator, we don't have any actual application for the new nuclear power plant, except for only one in Japan. And we have one application, experience to apply the gas turbine generator to the emergency power supply system, but only the one unit, okay.

So all the data come from -- and I mean this reliability data -- come from -- came from the actual industry application. So for example the starting system and some application used for DC, some application used AC power, and motor. And the other one, for example, the fuel system is different. And the breaker itself, different. And so it is very difficult to compare.

But it is very important, and when we do look at the data and also especially the failure, in the course of the failure, and if there is some failure mode which related to the breaker or some of those things, we need to analyze why those ones happen, and also we needed to reflect those variations to this calculation. That is my opinion

MEMBER BLEY: I'd like to suggest something to you. A few years back when there was an AEOD here at NRC, their staff published a series of risk studies looking at various items of equipment. They did one on emergency diesel generators, and it looked at the issue Mr. Stetkar raised, and showed the reliability of what would be inside their dashed line, and the test report compared to what one would need to analyze if one were doing a risk assessment, the larger set.

I recommend you take a look at that, because we are going to come back to this when we start seeing data later, real data.

MEMBER STETKAR: And as part of that, there are, I think, even in the 2007 -- in the 2007 data report it also breaks down the current diesel generator failure data, and you find that more than half of the failures that are included in the values that are quoted here for diesel generators are indeed failures of equipment that are outside the scope of what is being defined as a gas turbine generator. And yet there is still equipment that is relevant.

MEMBER BLEY: I think that is conservative.

CHAIRMAN MAYNARD: I think this is a real important point. I want to move on. I think a real key thing is for the staff, I think they hear our questions. And I think it is important that we are comparing apples to apples, and when we are talking about reliability data and so on. WE don't need an answer today. This is your informational brief. So I just think it's something when we come back to this for our review we are going to be interested in where does the data come from. How does it compare? Personally I don't think there has to be -- the gas turbine generator doesn't have to be significantly more reliable; just in the ballpark. A more important thing is, what's the data, and are we comparing apples to apples when we look at these things.

MEMBER BLEY: And it's not just whatever tests are going to be run; it's also where this industry data is coming from that you are using in other calculations.

CHAIRMAN MAYNARD: So this is a message as much for the staff as it is for MHI, and the questions that we are probably going to have in this area.

MEMBER STETKAR: To follow up, one thing you just mentioned, Dennis, and I didn't see it coming up in the slides, is that the Table D.1.0-1 of the gas turbine test plan is a reliability calculation. And it often relies quite heavily on numbers and I'm using my words carefully here, on numbers that are taken from IEEE Standard 500, which are known to be very optimistic compared to actual operating experience. There are several examples, solenoid valves, pumps, any mechanical equipment derived from IEEE Standard 500 tends to be a factor of 100 to 500 times more reliable than actual operating experience.

MEMBER BLEY: That whole study was a survey of experts from the industry -- not even experts, anybody who would contribute their thoughts.

MEMBER STETKAR: It was an Adelphi method of expert opinion, and it has been fairly well discounted by people looking at actual industry operating experience. So I only wanted to bring that up because Dennis is on -- certainly we are interested in looking at actual operating experience on the gas turbine units, but also within the reliability analysis that they have done, when you look at the sources of data that have been used, and how do those compare with data that are available from real operating experience on similar types of equipment -- solenoid valves, pumps, those kinds of things.

MR. PAULSON: Keith Paulson, could I ask a quick question of this issue so we can clarify it in our -- make sure our test program is consistent.

Are you saying that -- you are not saying that we have to have basically the same total functionality. What you are saying is, if you don't have the same equipment capability, that we're testing, you have to take that additional equipment into account somehow when you are coming into your final reliability.

MEMBER BLEY: I think I understand what you said. Those AEOD reports are a nice place to see it. If you can only test a subset, then when you compare you ought to compare only to that subset. Everything outside of that would need to be modeled.

MR. PAULSON: Yes, that was my

question.

MEMBER STETKAR: When you model it, make sure that you use data from similar equipment and experience.

MR. PAULSON: Right, that's critical for us because what we are testing is pretty well defined right now. But as long as we have a way to adjust for the complete package, so that so to speak breaker to breaker. You know what I mean, front to back, that we are comparing apples and apples.

CHAIRMAN MAYNARD: Let's go ahead and move on.

MR. NIIDA: This slide I've already explained, the reliability target for 1E GTG. Next, we show GPS6000 satisfies the requirements for US-APWR by using Bayesian approach. The first estimate of GPS6000 will be performed by updating the known informative flyer with GPS operational data . And you know the Bayesian approach is one of the general methods of study. And it is widely used to evaluate component reliability and its uncertainty. NUREG-CR/6928 also uses this approach.

Recognizing HAZMAT PRA standards as

preferred method for component data analysis. I know that to estimate GPS6000 very accurately, collection of data based on appropriate categorization is necessary. And we have analyzed available and relevant GPS's operational data. And operational data have been collected from manufacture's record as shown in, next, Table 1.

This table, this is a product number rated output and single engine or twin engine and fuel type and starting system type. And each number of starts and number of failure.

And next table continue. We corrected this. And GPS series have been produced with common design concept such as structure, and dynamic characteristics and materials. And increasing of output is achieved to size up the design of small product analogously.

And the near output products have more similar design. And MHI apply GPS6000 as EPS. And GPS5000 is similar design as GPS6000.

Also GPS4000 and 4500 almost same design as GPS6000. And these are no significant difference of starting capabilities based on operation experiences.

Another mean of increasing output is

using two engines with one generator. Over GPS2000 products are twin type all. Starting type is also considered whether air or DC motor.

MHI has selected the data in Table 1. Data of GPS4000 to 6000 with air starting type, 1433 demands with zero failure.

This data is used to Bayesian approach of GTG reliability. Next from the point of running reliability, type of studying system is not needed to consider. Also there are no significant difference from operation experiences of large output twin engine products of over GPS2000. And we have classified data into running time of over GPS2000 and running time over GPS4000.

The result of this data of over GPS2000, 3820 was with zero failure. And the data of over GPS4000, 2224 hours with zero failure.

The result of this, we evaluate both above GPS2000 data and GPS4000 data. Both are considered proper to use to Bayesian approach. However, we evaluate using only data for GPS4000 only conservatively.

Reliability estimation with GTG based on industrial operation experience. I've explained applicable data of 1433 demands with zero failure, and 2224 long was with zero failure.

The result of this, uncertainty over failure rate or probability estimated by posterior distribution for Bayesian approach.

MEMBER BLEY: I have a question. I don't see it here, and I don't recall reading this maybe it's somewhere that I missed. Eventually, you don't need to show me today, but we'd be real interested in knowing what the prior is that you used. And I think I would agree that a Bayesian approach is best, but it is highly dependent on the prior distribution you use, and we would -- expect us to look at that . And I hope staff takes a good look at the prior. It should be well justified prior. Or not informative, one or the other.

MR. NIIDA: And from these data it is divided as shown in Table 2. Probability to fail to start is regulated by 3.5 time 10 to the minus four. And the probability of fail to run is evaluated is 2.2 times 10 to the minus fourth power.

And next, this slide shows posterior distribution of GTG reliability. Distribution of fail to start, and distribution of fail to run.

Next --

MEMBER STETKAR: Sorry, I was trying to find a reference, perhaps you can help me. I thought that I recall reading in a response to one of the RAIs that the operating experience data on not this precise gas turbine generator but other gas turbine generators that are in service, he showed two failures to start. And I was curious how your Bayesian updates accounted for that operating experience. Or were those failures determined to be not valid for some reason?

MR. KAWANAGO: In the beginning, in our technical record, we calculate the reliability data by using our Kawasaki gas engine carburetor as experimental start time. So we calculate to failure divide total is 7,394 start time. But we -- as you know we got the RAI from the NRC staff, and that approach itself it's a very difficult to repeat the architecture of --- to calculate the actual and reliability.

So -- and go back to this table, and we -- initially it's in our technical report -- and the reliability and data is so wide, from the 100 KVA to the 6000. But we selected the appropriate range, and also from this data, and as Niida San explained to you, we have some selection additionally. I mean the twin or one engine or the air start issue. And so our conclusion, and we used from the 4000 KVA to 6000 KVA, and so I think those data come right to the -- after the calculation, the reliability data for this component.

And so we think easily fit to the actual distribution.

MEMBER BLEY: I guess I was just going to take us back to where we were awhile ago. Those old 8D reports broke the whole system into a number of boxes. And the one thing they demonstrated was that for some of those boxes, all your data are probably applicable; and for other ones, only some of the data are applicable. It lets you make maximum use of all the data without throwing away some that might have failure modes that even though the machine is not quite like yours are appropriate for consideration. So you need to be careful about that. And I can't comment on the details of what you just said, because I haven't seen them. But you need a good rationale, especially if there are failures that you are censoring from the data, why those failure modes aren't applicable to your machine.

We don't have large amounts of data here to work from.

MEMBER STETKAR: And the data in particular that were cited, whether they are applicable again, my question was, what type of process was used to determine that those particular data are not applicable. But the numbers that were cited there were things like failures in 75 demands, and failures in 120 demands, which -- it's not clear if you looked at variability among the population, if they are relevant failures, how that might affect a Bayesian update approach from some prior.

So I think it's important to -- as Dennis mentioned -- to understand why those particular failures are not relevant for the evaluation of these particular engines.

MEMBER BLEY: Just one last thing. It's tempting to censor failures we don't think were applicable, so you need to be careful about that. But if you are going to censor some of it, there are probably a lot of successes you ought to be censoring on the same basis. So you can't just throw away the bad stuff.

MR. SPRENGEL: And that's true. I mean he referenced 7000 starts was the original. So I mean it has been scaled down in both respects.

MR. KAWANAGO: I'm sorry, I want to gripe again. And through selecting the actual job and the data set, and we explained to you, and the total is 401433-demand with zero failure. And we don't -- and we don't eliminate intentionally the two failures. I mean it is -- how do you say it? -- there is the true failures. However those ones are over, the other range of the product is 100-1000 KVA or something like that.

And so, through the process of selecting the appropriate range of altitude and those type of ending and starting system. And finally those two failures were excluded.

MEMBER STETKAR: No, I understand the process. And I see it used a lot. That does not necessarily mean, to me anyway, that the two failures are not relevant, just by restricting the population to a smaller set with a smaller number of demands with no failures.

CHAIRMAN MAYNARD: I'd like to move

on, and it's more important to get to some of these other things. I think it is something that we will have a lot of interest in when it comes time for our review of the task review on this. Let's go ahead and move on.

MR. NIIDA: Let's form these out of to Table 2. We want to say, to start this, that operational experience shows that failure rate is low, while the mean failure rate of the DGs with 95 percent confidence. And starting tests we performed as a typical qualification starting test. Total starting times is 100, Bayesian, and reliability will be updated by the starting test and the surveillance test we obtained during plant operation.

Next for run test, operational experience shows that failure rate is lower than the failure rate of DGs with approximately 95 percent confidence. And a run test is not needed.

And reliability we performed and updated by the surveillance test we also obtained during plant operation. Next, we summarized the liability. First, based on limited test data, GTG reliability appears to be capable of exceeding reliability assuming PRA analysis.

In addition to MHS PRA reliability target, we should satisfy with reliability requirement Reg. Guide 1.155. Reg. Guide 1.155 requires all 0.95 or 0.975 reliability with 95 percent confidence.

If we get -- if we set the target case zero point nine five, we will perform 100 startup test.

If we set target case of zero point nine seven five we will perform 150 startup tests.

MEMBER ABDEL-KHALIK: If you go back to the previous slide, you make the argument that run test is not needed based on comparison with diesel performance. But given the issue that was raised by Mr. Stetkar earlier regarding the boundaries of your system vis-a-vis what we define as a diesel engine, wouldn't you have to reconsider that assessment?

MR. KAWANAGO: Basically we understand your point, and however, I think and we have as you know two approaches. One is the diesel calculation. And those we checked after the failure mode--I mean as compared to failure mode--and so we think, and this calculation itself is enough to get preliminary and the --

(Unintelligible due to Asian accent combined with technical terminology, hereafter referred to as UDTAACWTT.)

-- of the reliability in addition. And we have a type test with which we conducted the 100 times -- the 100 start test or 150 start test.

And so those combinations, I think, we don't need to have the reconsideration --

MEMBER ABDEL-KHALIK: I'm sorry, I don't understand your argument. Why would 100 start tests or 150 start tests negate the need for run tests.

MR. NIIDA: For run tests? Okay, for run tests.

MEMBER ABDEL-KHALIK: Right.

MR. NIIDA: Okay, I understand. I'm sorry, I misunderstand start test. So your question is run test?

MEMBER ABDEL-KHALIK: Yes.

MR. NIIDA: I understand. Basically when we talk about the run tests, and what these main failure mode of the failure of the alarm itself, it is very important. For example when we talk about fail to start, there are so many, it's a distributor for the fail to start: it's an AR-system failure, what to think? But when we look at the fail to run, the main contributor is the engine and generator itself. We don't care, we don't care after the starting system, we don't care the fuel apparatus system -- maybe, maybe sometimes they contribute. But we don't think, and now when we look at the actual data, and it's a total of 38, 20 hours with zero failure, 22, and 24 hours with zero failure, if there is a one failure, two failures, and so on, we need to think about what is the root cause. But now it's at zero failure, that means engine and also the -- it's a generator --

MEMBER ABDEL-KHALIK: But it seems to me that all you are saying is just conjecture, because you have not looked at the difference between what you define as your system boundary and what is typically defined as the boundary of the EDG system .

MR. KAWANAGO: Especially when we focus on the failure to start.

CHAIRMAN MAYNARD: I'd like to go ahead and move on. I think the staff has heard the question. Again, we don't need to resolve issues here today. I think we kind of raise some questions so you will know what we will be looking at.

I'd like to go ahead and move on because we are running low on time here?

MR. KAWANAGO: May I? And that's it.

CHAIRMAN MAYNARD: I don't think we need to go through the details of each slide here. I think if you can kind of summarize some things.

MR. KAWANAGO: Okay. The next slide, Class 1E Qualification Plan. And we will perform Class 1E Qualification --

(UDTAACWTT.)

-- based on EPRI 5652. This is guideline of the Commercial dedication process.

Testing will be preformed by IEEE 387 under Reg. Guide 1.9. And the seismic qualification will be preformed by IEEE 344.

We submit developed education report consisting of this content.

There are three type tests, capability test, and the startup and load up system test, and the module tests.

And this slide shows our qualification schedule. We will finish qualifications including test until end of next year.

MEMBER BLEY: Will the qualification testing, does that all need to be finished before the design cert? Or is that a COL item?

MR. SCAROLA: I think we are completing the testing before design certification.

MEMBER BLEY: And that's part of design certification? Thank you.

CHAIRMAN MAYNARD: Let's go ahead and we'll move on. I note some uncertainty here, but it's not important that we have that defined immediately. We will certainly know when we get to the DCD review.

MR. NIIDA: From this slide I explain about the AAC-GTGs. US-APWR two AC power sources which apply known safety rated gas turbine generators.

Under this one, I have already explained. These are two AAC gas turbine generators.

And this AAC GTGs use under the SBO condition.

Next, this slide shows a specification for AAC GTG. AAC GTG is a known safety rated and two units and 4,000 kilowatt continuous output.

And this shows power supply and each condition for onsite for system. First one is under the normal operation. And next is definition SBO. SBO refers to complete loss of water. And the next slide shows flow.

MEMBER BLEY: You skipped a couple of slides, and I guess they have to do with this. The station blackout definition, the 1E gas turbines, and it appears the argument that you don't take these out as well is that they have a different kind of starting system and are somewhat different machines that have different capabilities. Is that the argument?

MR. SPRENGEL: There is a diversity argument, yes.

MEMBER BLEY: Okay, and the diversity has to do with --

MR. SPRENGEL: We will touch on that some more.

MEMBER BLEY: Okay.

MR. KAWANAGO: Safety conditions can be achieved by AAC.

And this slide shows this configuration of AAC and buses. Usually AAC is connected to non-safety related buses. Under AAC, this switched to Class 1E buses and backup.

MEMBER STETKAR: This drawing here indicates that each AAC gas turbine will have three output circuit breakers. Is that the actual design? So there will be three separate output circuit breakers?

MR. KAWANAGO: But only the manual control.

MEMBER STETKAR: Thank you.

MR. NIIDA: This is summary. AAC is started within 100 seconds and plant safety conditions for minimum eight hours. But AAC fills storage tank, and has seven days operation. And on this slide I explain diversity between EPS and AAC.

MEMBER ABDEL-KHALIK: The statement regarding the reactor coolant pump seal, the integrity of the reactor coolant pump seal can be maintained for eight hours without cooling, do you have data to support that?

MR. KAWANAGO: I think it is basically we wrote in here eight hours, but actually in our application AHE comes -- power supply within one hour. And so --

MEMBER ABDEL-KHALIK: No, no, no, I'm just looking at this statement the way it is written. Reactor coolant pump seal can be kept -- can maintain its integrity for eight hours without cooling. Do you have data to support that?

MR. KAWANAGO: We can show you the data for the one hour. Because basically a standard point was created for the safety analysis. Only we use the one hour.

MEMBER BLEY: So you are not vetting this statement? You are saying maybe it won't last eight hours?

MR. KAWANAGO: On, no, no, no. My point is --

MEMBER BLEY: I understood that. But is this statement true or false?

MR. KAWANAGO: In actual Japanese test data, and we can show you the eight hour data.

MR. SPRENGEL: So yes.

CHAIRMAN MAYNARD: You have data to show eight hours? Okay.

MEMBER ABDEL-KHALIK: Then we really would like to see that.

CHAIRMAN MAYNARD: But you are only

taking credit for one hour, is that --

MR. KAWANAGO: That's right.

CHAIRMAN MAYNARD: Okay.

MEMBER BLEY: What kind of seals -- oh, well, we'll get into that.

CHAIRMAN MAYNARD: That's a different chapter.

MR. KAWANAGO: The time basis is one hour.

MEMBER ABDEL-KHALIK: I understand, but you are making a statement here that these things last for eight hours without coolant. And we are trying to find out whether this is true or false, and what is the basis for it, and where are the data.

CHAIRMAN MAYNARD: But I think that is for another chapter. We will certainly get into it.

MR. NIIDA: From this slide, diversity between EPC and the AAC-GTG. First, AAC-GTG should be designed to minimize potential CCF between GTG.

Next, now on the proceeding two approaches, two solutions. One is we use different manufacture products. In this case design issue and diversity between the AAC-GTGs. The other solution is we use same manufacture. But in this case the variation diversities is resolved by using analysis.

MEMBER BLEY: Will these be using diesel oil as well? Will these be using diesel oil as fuel as well?

MR. SPRENGEL: Yes.

MEMBER SIEBER: Yes.

CHAIRMAN MAYNARD: They will run on about any thing.

MEMBER BLEY: Run on about anything, but what I was getting at we have had some failures of deliveries of bad oil that affected multiple machines. But these will use the same fuel oil as the diesel?

MR. KAWANAGO: That's right.

And we are now on the preceding condition. Now this approach two.

MR. SPRENGEL: From here on out we are talking about approach two, so the discussion is different if we select a different manufacturer. That evaluation is ongoing. So from here on out it's the second discussion.

MR. NIIDA: This is a sample

regulation. In this case the first one is GPS6000 is applied for GTG. Thirty-three is engine serial number of the GPS6000. On the other hand GPS4000 is applied to AAC-GTG.

And we evaluate -- we divided each portion and we collect each difference of each equipment and components.

Basically GPS6000 and GPS5000 basically engine portion is almost similar to each other. But the supporting system is different and the components are different.

This table also shows supporting system. Supporting system components and equipment are different each other completely.

MR. KAWANAGO: So our point is basically the -- and we have so many data related to the failure of the start of the diesel generator, and --

MEMBER BLEY: Can I ask a quick question on your last slide? You don't have to pull it up. Of those starting motors, you have eight of them on there, this is ASE, how many of those need to function to start the machine, it's on slide #57. Eight starting motors. How many actually have to work to start the machine? All of them?

MR. KAWANAGO: To keep the starting time within the 100 seconds, we need to have these eight motors. And if we only used two motors, and so, starting time would expand, 200 or 300. However --

MEMBER BLEY: But it will still start?

MR. KAWANAGO: Yes.

MEMBER BLEY: Thanks.

MR. KAWANAGO: So we would like to conclude this presentation. We have the main data for the code. And so now we are under estimation and evaluation the -- how we can eliminate the common cause failure by using our evaluation, for example, that this one shows. And the code is under ING system failure, was generator failure, and so on. And so when we go to the contributions of the gas turbine generator, and by using the actual experience, we need to have the diversity of the system, and we need to have the diversity of the generator and we need to have the diversity. And those evaluations will be now under proceeding.

But again, we have two approaches.

One is different manufacture. The other one is the same manufacture and we are now under the proceeding aberration. That's all.

CHAIRMAN MAYNARD: Thank you. Any questions?

I'm going to ask for public comments here in just a minute if we've got them. Appreciate the presentation here.

I think some of the key things that we've talked about, the data and comparing apples to apples. I don't think it's so important to show that it's a lot more reliable; I think it's more important to show that the numbers that you are showing, what do they really compare to, and what's -- where does that data come from?

The other thing I think is going to be very important is understanding -- you have like the one unit, you've got two turbines, and you've got multiple starts, how many of those things are going to need to operate if all of them, that's fine, if not, it's kind of like, if part of it fails does that mean the whole thing fails?

I think that is some of the other things we are going to want to get into in our discussion when we review this as part of the DCD review.

With that do we have anybody from the public who wants to make any public comments?

If not, I'd like to go ahead and draw the morning session to a close. I'd like to ask the staff, I would like to start the afternoon session early if you can have the -- I don't know if Royce could be here or not. It's a closed session. As long as we have the people here that are needed from the staff and the applicant, we can start that early.

So what I'd like to do, we will start back in session at 12:45, and we will come into closed session at that time. So we will recess for lunch.

(Whereupon at 11:46 a.m. the proceeding in the above-entitled matter went off the record to return on the record in closed session at 11:50 p.m.)

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

US-APWR
Standard Design Certification
Gas Turbine Generator Overview

To:
Advisory Committee on Reactor Safeguards

By:
Ngola Otto, Project Manager
U.S. Nuclear Regulatory Commission

Thursday, May 21, 2009

Purpose

- Provide status of the NRC staff review of US-APWR Design Control Document (DCD) Chapter 8, DCD Sections 9.5.4 – 9.5.8, and the following Technical Report referenced by the DCD:
  - Qualification and Test Plan of Class 1E Gas Turbine Generator System, MUAP-07024-P(R0), dated December 2007
- Address the Committee’s Questions

Gas Turbine Generator Applicability

- Use of 4 Gas Turbine Generators as safety-related, class 1E onsite power source for US-APWR Design
  - use as a safety-related emergency power source is a first of a kind Nuclear Power Plant (NPP) application
- Use of 2 Gas Turbine Generators (GTGs) as alternate AC power source for US-APWR Design
- Reliability of GTGs to meet RG 1.155 Station Blackout rule of 0.95 minimum
- Diversity of GTGs to meet commission's guidance in SECY 90-16 for use of GTGs as alternate AC power source

Design Review Status

- RAIs have been issued and responses have been received
- Teleconference meetings conducted in March 2009 with MHI to address issues
- Public Meeting on April 13, 2009 to address GTG reliability and diversity
- Additional RAIs to be issued

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Design Review Status

- MHI will provide to NRC its diversity strategy based on public meeting discussion conducted on April 13, 2009
- MHI will provide a revised Technical Report (MUAP-07024-P) to address RAI questions
- GTG review will be included in Chapter 8 and Sections 9.5.4 - 9.5.8 Safety Evaluation Reports

Summary

- Design review currently being conducted by NRC staff
- MHI will conduct 100 initial type tests with no failures per IEEE 387 to demonstrate with 95% assurance that the safety related GTGs meet 0.95 reliability required for RG 1.155 (Station Blackout)

United States Nuclear Regulatory Commission

Protecting People and the Environment

US-APWR Topical Report MUAP-07006 Defense-in-Depth and Diversity Safety Evaluation Report

To:
Advisory Committee on Reactor Safeguards

By:
Jeff Ciocco, Senior Project Manager
U.S. Nuclear Regulatory Commission

May 21st, 2009

Purpose

- Provide an overview of the licensing review of the Defense-in-Depth and Diversity (D3) Topical Report

- Address the Committee's questions

Defense-In-Depth and Diversity (D3)

- D3 is one of four topical reports that make up the generic portions of the MHI digital I&C Design. The other topical reports are:
  - Safety I&C System Description and Design Process
  - Safety System Digital Platform - MELTAC
  - HSI System Description and HFE (Human Factor Engineering) Process
- Topical Report requests approval of the D3 approach for the US-APWR & is referenced in Chapter 7 of Design Control Document

Licensing Process

- Acceptance Review conducted 2007
- Acceptance Letter issued December 2007.
- D3 not reviewed for operating reactors.
- RAI’s Issued May 2008
- RAI Responses received October 2008

Licensing Process (cont'd)

- Informational Briefing to ACRS Subcommittee in November 2008
- Send draft D3 SER to MHI to technical adequacy review
- Present D3 SER to ACRS US-APWR subcommittee
- Present D3 SER to ACRS full committee
- Finalize D3 SER

Summary

- D3 SER delivered to ACRS
- Presenting D3 SER to subcommittee and full committee

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

US-APWR
Diversity and Defense-In-Depth
Topical Report
Safety Evaluation

To:
Advisory Committee on Reactor Safeguards

By:
Royce D. Beacom
Instrumentation, Controls and Electrical Engineering Branch (ICE1)
Office of New Reactors

Thursday, May 21, 2009

Agenda

- Background
- Diversity and Defense-in-Depth Scope
- Significant Requirements, Standards, Polices and Guidelines
- Findings and Conclusions
- Application-Specific Actions Items

Background

The generic portions of the MHI digital I&C design is described in four topical reports:

- Safety I&C System Description and Design Process
- Safety System Digital Platform - MELTAC -
- HSI System Description and HFE (Human Factor Engineering) Process
- Defense-in-Depth and Diversity (this topical report)

Diversity and Defense-in-Depth Scope

- New reactor design only – US-APWR
  - (MHI intent was for Operating Fleet also)
- Diversity with Safety and Non Safety Systems
  - Protection and Safety Monitoring System (Safety)
  - Plant Control and Monitoring System (Non-Safety)
- Both using the MELTAC Platform

Diversity and Defense-in-Depth Scope

- Functionality of the Diverse Actuation System (DAS) – (analog & non-safety)
  - Provides a defensive measure to cope with Anticipated Operational Occurrence (AOO) or Postulated Accident (PA) concurrent with Common Cause Failure in the PSMS which is beyond design basis

Diversity and Defense-in-Depth Scope

- Provides the ATWS Mitigation Function
- Provides Automatic Actuations where time is insufficient for manual operator action; MHI Proposed: < 10 mins
  - Delay from anticipated PSMS trip
  - Proper actuation of PSMS blocks DAS

Diversity and Defense-in-Depth Scope

- DAS Manual Actuation
  - Separate HSI Panel with conventional Controls and Indicators
  - Proposed < 30 min from Prompting Alarm
- Isolated signals from sensors, shared with PSMS, provided to Non-Safety DAS
- DAS Outputs to discrete portion of Power Interface Module (PIF)

Acceptable Bases for Implementation of Requirements in the D3 Approach

- SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs"
- SRP Section 7.8, "Diverse Instrumentation and Control Systems"
- SRP Branch Technical Position (BTP) Instrumentation and Control Branch (HICB)-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems"
- NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems"
- GL 85-06, "Quality Assurance [QA] Guidance for Anticipated Transient Without Scram (ATWS) Equipment that is not Safety-Related"

Findings and Conclusions

- LBLOCA Coping Strategy
  - High quality, high reliability, measures of MELTAC within the RPS/ESFAS design
  - Low frequency of AOO and PA events
  - Supplemented with DAS leak protection
- LBLOCA Strategy unacceptable
  - Frequency of AOO / PAs still finite possibility
  - Application of LBB is not applicable

Findings and Conclusions

- Protective action – Manual vs Automatic
  - MHI "Target" $\leq$ 10 minutes - Automatic
  - > 10 minutes – Manual Action is assumed
    - Differs from DI&C-ISG-02; < 30 Minutes – Auto
    - Insufficient information to assess manual action between 10 min and 30 min following the event
- Justification for manual actions within 30 minutes – US-APWR HSI Certification

Findings and Conclusions

- The staff concluded that the D3 approach, and the D3 analysis provided per NUREG-6303, had met the acceptable bases for conforming to the requirements and supporting industry standards.
- Subject to satisfactory completion of Application Specific Action Items (ASAI)

Non-Proprietary

Application Specific Action Items

1. Applicant shall demonstrate the that the isolation devices are conventional (e.g., non software based devices) and completely testable in order to meet the independence and isolation requirements of IEEE Std 603 and address fault-isolation criteria of IEEE-384
2. Applicant shall demonstrate the acceptability of all manual actions. Also, the concept and application-specific implementation of the priority alarms should be adequately demonstrated.

Application Specific Action Items

3. Applicant shall demonstrate that the PIF Module is not susceptible to a software CCF.

4. Applicant shall identify the specific controls and indications for the DHP and address human factors aspects for the DAS and PSMS system-level manual actuation means.

Application Specific Action Items

5. Applicant shall provide the final determination of the setpoints and the response time of the DAS.
6. Applicant shall demonstrate that the acceptability of the QA process used for the DAS meets the guidelines of GL 85-06.

Application Specific Action Items

7. For each AOO in the design basis occurring in conjunction with each single postulated CCF applicant shall demonstrate that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10 percent of the 10 CFR Part 100 guideline value or violation of the integrity of the primary coolant pressure boundary.

Application Specific Action Items

8. For each PA in the design basis occurring in conjunction with each single postulated CCF, the applicant should demonstrate that the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding the 10 CFR Part 100 guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits).

Application Specific Action Items

9. Applicant shall address the partial failures of the PCMS/PSMS and demonstrate an adequate D3 strategy to cope with such failure modes
10. Applicant shall provide an acceptable defense in depth and diversity strategy for a LBLOCA concurrent with a CCF of the PSMS.

Application Specific Action Items

11. Applicant shall submit all the information indentified in Section 10.0 of the topical report, “Future Licensing Submittals.”

US-APWR

GAS TURBINE GENERATOR (GTG)

used as Emergency Power Supply

May 21,22 2009

Mitsubishi Heavy Industries, Ltd.

Presentation Summary

Class 1E GTG

- Introduction
- Background
- GTG Advantages & Disadvantages
- Requirement, Design concept and Specification
- Onsite AC Power System
- Applicability for US mainly codes, standards
- Load Sequence
- Starting Capability
- Reliability
- Supporting System of GTG
- Control and Protection of GTG
- GTG System
- Class 1E Qualification

Presentation Summary

US-APWR

AAC-GTG

- Introduction AAC-GTG
- Onsite AC Power System
- Design Basis of AAC-GTG
- Requirement, Design concept and Specification
- Power Supply to Onsite Buses
- Operation under the SBO
- Diversity

Introduction(1) *Class 1E GTG*

- The US-APWR uses Gas Turbine Generators (GTGs), as Emergency Power Supply (EPS) in lieu of the commonly used Diesel Generators (DG).
- The reasons for the selection of the GTG are as follows:

  a. The Gas Turbine is a very simple rotating engine with few components

  b. The GTG System consists only of the gas turbine, generator, fuel transport, starting and control/instrumentation systems

  c. Water cooling system is not required

  d. The GTG presents a high level of reliability.

Introduction(2) *Class 1E GTG*

- In the case of the application on gas turbine generator system for nuclear power generation, should be considered high reliability and capability. To meet this requirement, the combination of an extremely reliable aircraft component with equally reliable industrial components such as reduction gears, electrical generator, governor, voltage regulator, relays and similar components is selected. The advance accumulator design of the US-APWR allows a starting time for the GTG of under 100 seconds.

GTG Advantages & Disadvantages(1) *Class 1E GTG*

US-APWR

	Gas Turbine Generator	Diesel Generator
Space	Compact	Large
Cooling Water	Not Required	Required
Periodic Maintenance	Required less than DG	Required
Reliability	Expected to be Better than DG	10^{-2} (/d)
Starting Time	40 sec	10 sec

GTG Advantages & Disadvantages(2) *Class 1E GTG*

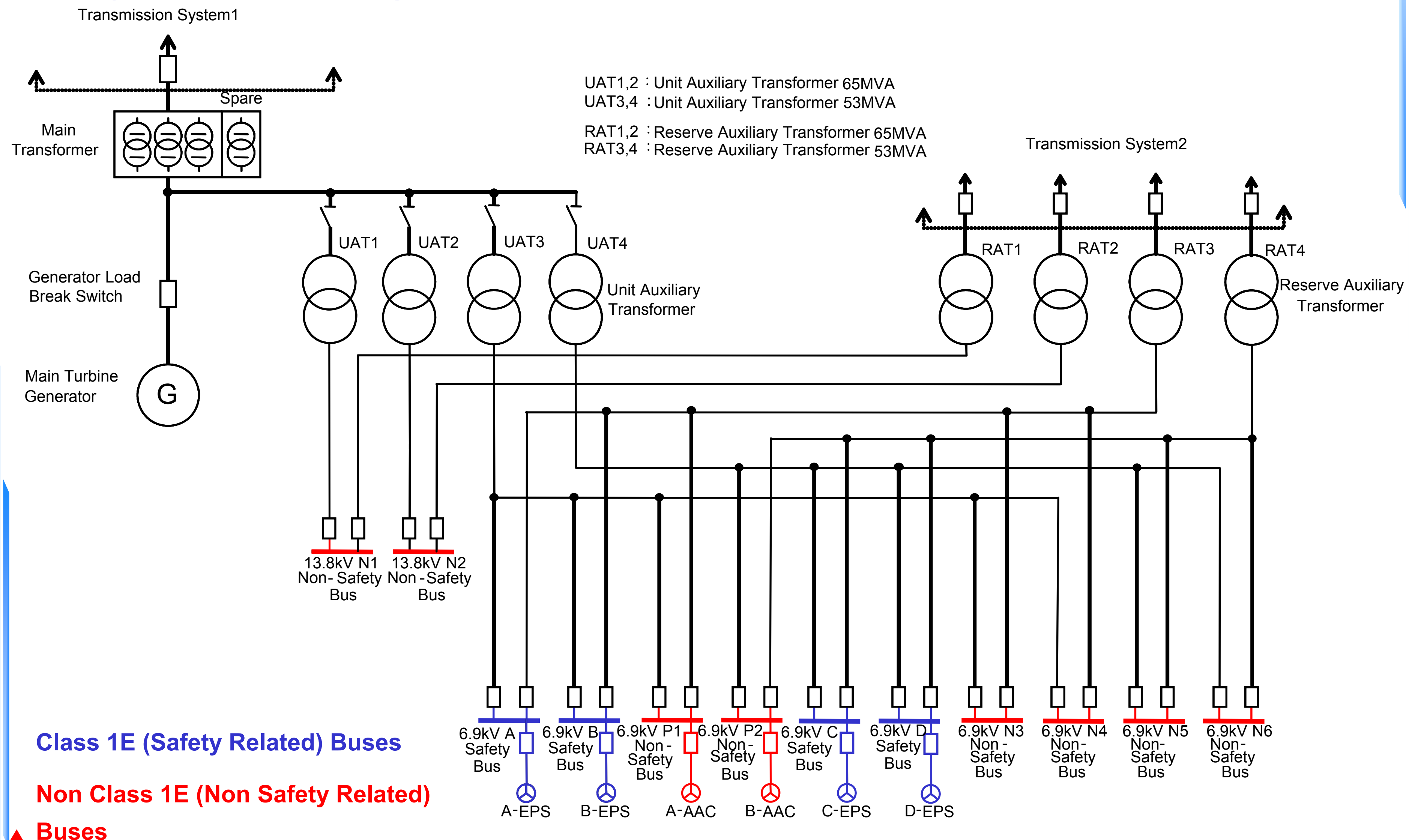
US-APWR

	Gas Turbine Generator	Diesel Generator
Noise level	High Freq levels are ease to silence	Noisy
Vibration	Very small levels, because the engine is not reciprocating	
Power Supply	Frequency variation is small	+/- 2% Frequency variation
Exhaust Gases	Low levels, since the combustion efficient is high	

Onsite AC Power System *Class 1E GTG*

US-APWR

➢System Configuration



Requirement, Design concept and Specification
Class 1E GTG

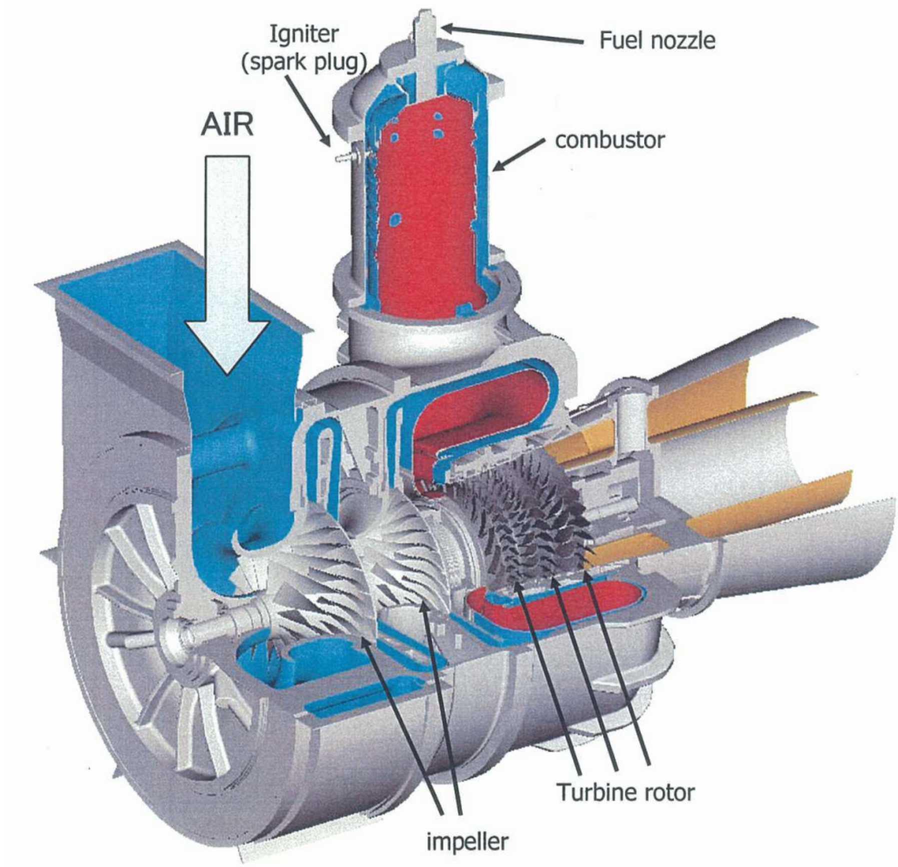
US-APWR

➢ Design requirement, Specification of EPS

- ✓ Class 1E, Seismic category 1
- ✓ Four 50% units
- ✓ 4500 kW Continuous @ 1,000 hrs Engine Overhaul Interval, 115° F Air Intake Temperature
- ✓ 4950 kW Short Time @ 300 hrs Engine Overhaul Interval, 115° F Air Intake Temperature
- ✓ 6900 V, 3-phase, 60 Hz
- ✓ Air starting type, air receivers of each train have capability to start the GTG for three time.
- ✓ Fuel: Diesel oil, fuel storage tank of each train has capability to operate the GTG during seven days under continuous rated capacity. Fuel day tank of each train has capability to operate the GTG during 1.5 hours under continuous rated capacity.
- ✓ Class 1E GTG should satisfy with requirements of voltage/frequency variation required in R.G 1.9.

GTG System(1) *Class 1E GTG*

Engine

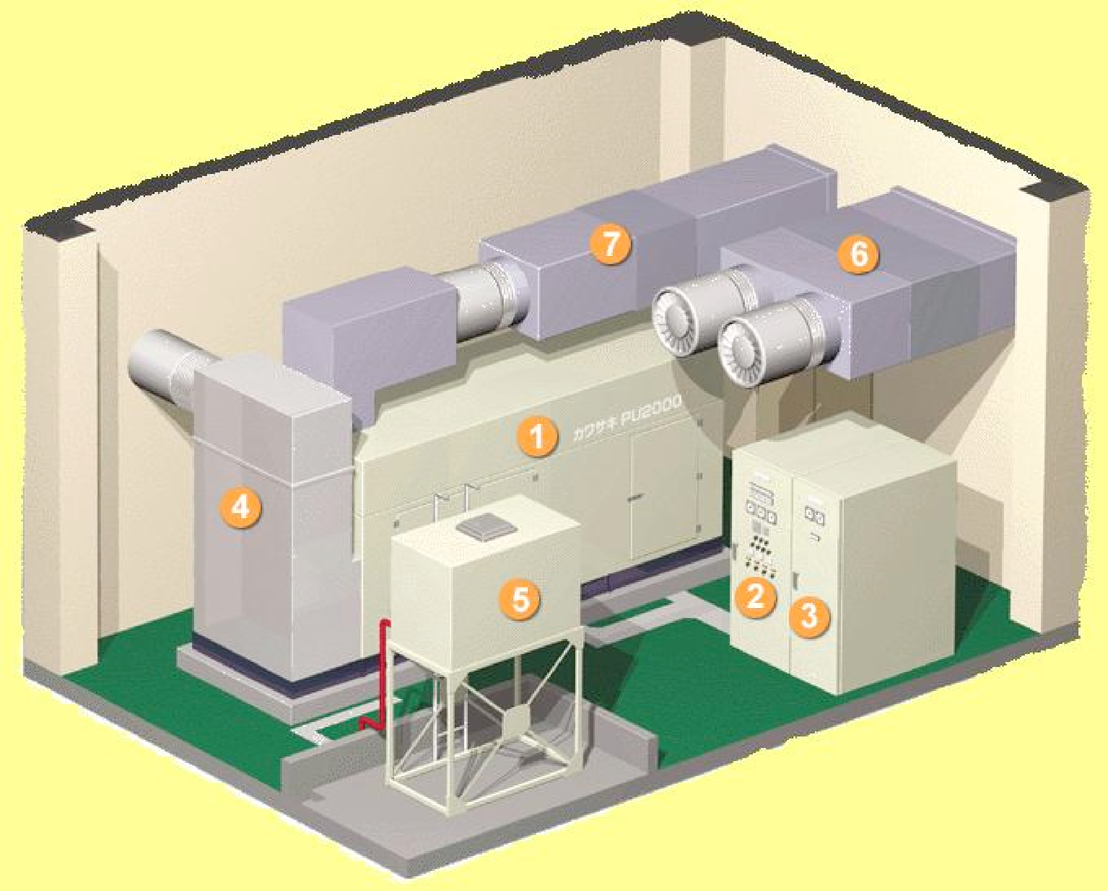


M1A-33Gas Turbine

GTG System(3) *Class 1E GTG*

US-APWR

TYPICAL SYSTEM LAYOUT



① ***Gas Turbine Package***

Includes gas turbine and generator with an acoustic enclosure .

② ***Control Panel***

Includes gas turbine and generator control panels.

③ ***Battery Panel***

Includes battery and charger.

④ ***Exhaust Silencer***

⑤ ***Liquid Fuel Service Tank***

⑥ ***Ventilation Intake System***

Includes fan and silencer.

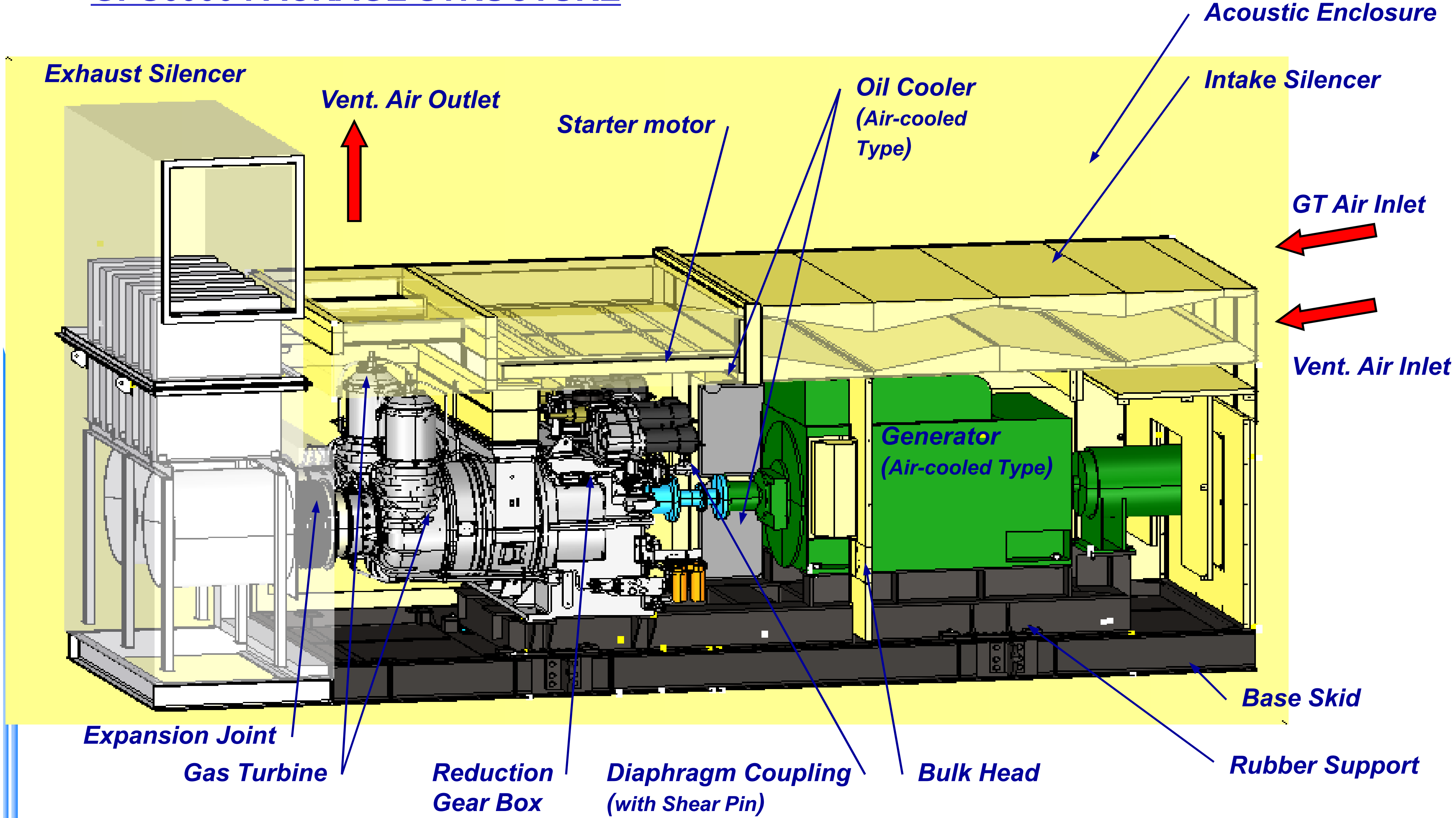
⑦ ***Ventilation Exhaust System***

Includes fan and silencer.

GTG System(2) *Class 1E GTG*

US-APWR

GPS6000 PACKAGE STRUCTURE



Supporting System of GTG *Class 1E GTG*

Supporting system of GTG (1)

System	Diesel Generator System	Gas-Turbine Generator System
Fuel System		Fuel system of GTG is almost similar to DG's. Fuel system is designed based on requirement for safety-related EDG system.
Lubricant System		Amount of consumption of lubricant oil is less than DG's. System is simpler than DG's and system components are fewer than DG's. Lubricant system is used for both engine and generator. Also pre-heat of lubricant oil is not needed.
Starting System	Compressed air rotates the engine directly.	Stating air system of GTG is almost similar to DG's. Air-motors rotate the GTG. Starting system is designed based on requirement for safety-related EDG system.
Cooling System	Water cooling, pre-heat is needed for quick start.	Water cooling is not needed. Self ventilation fan can cool engine and generator package.

Supporting System of GTG *Class 1E GTG*

US-APWR

Supporting system of GTG (2)

System	Diesel Generator System	Gas-Turbine Generator System
Inlet/Exhaust air system		Inlet/Exhaust air system consists of ducts, fan and exhauster. Inlet air is used for both combustion and ventilation. Vented air is discharged, and exhaust is discharged via the exhauster/silencer.
I&C		✓Governor and AVR control is similar to DG's. Monitoring parameters, protection signals are differ from DG's. ✓Control logic of GTG is designed special to GTG, and logic is installed in Class 1E control cabinet.
Auxiliary Power		Auxiliary power is designed almost similar to DG's. ✓Pumps, fans are supplied power from Class 1E ac 480V plant power system. ✓Starting air valves, excitation of generator, control circuits are supplied power from Class 1E dc 125V plant power system.

Control and Protection of GTG(1) *Class 1E GTG*

US-APWR

Start up(1) *Start Signal*

Starting logic is designed to satisfy with requirements for safety-related EDG system. The Class 1E GTGs are started by following Methods.

- ✓ Automatic starting by the ECCS signal
- ✓ Automatic starting by an undervoltage signal and degraded voltage signal on the Class 1E MV bus to which Class 1E GTG is connected
- ✓ Manual starting from MCR
- ✓ Manual starting from the GTG room
- ✓ Manual starting from the remote shutdown room

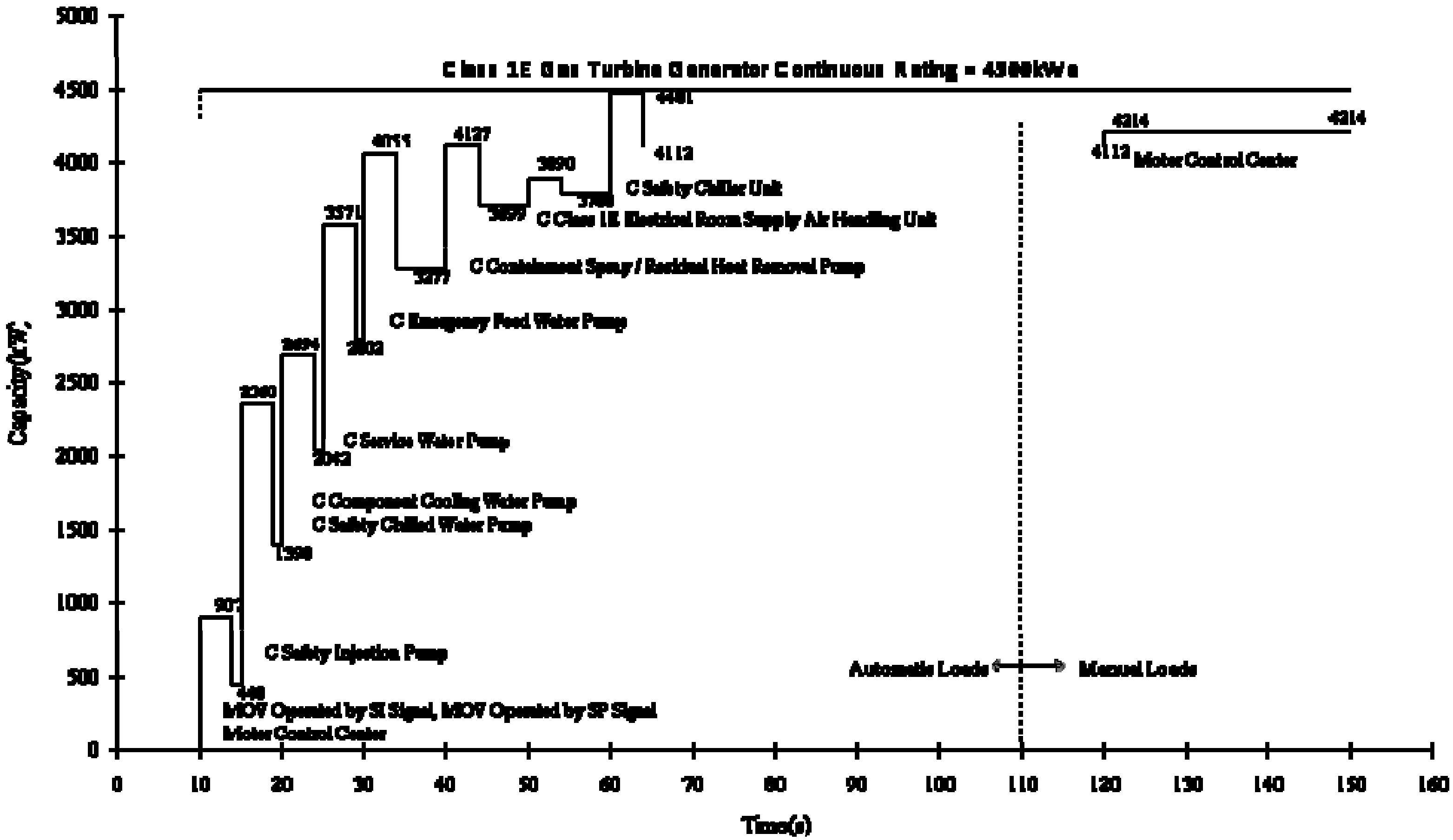
Start up(2) *Starting Time*

- **Starting Time**
  - ✓ (1) Starting time of GTG is required within 100 seconds by safety design and analysis of US-APWR. For GTG to reach set voltage and frequency, and GTG breaker should be closed within 100 seconds after starting signal is initiated.
  - ✓ (2) GPS 6000 can reach set voltage and frequency within 40 seconds as its standard specification.

Control and Protection of GTG(3) *Class 1E GTG*

US-APWR

Start up(3) *Load Sequence*



Control and Protection of GTG(4) *Class 1E GTG*

The following trip protective functions are provided during operation of the Class 1E GTG.

- ✓ Overspeed
- ✓ Generator differential current
- ✓ High exhaust gas temperature
- ✓ Failed to start
- ✓ Overcurrent
- ✓ Low pressure lube oil
- ✓ High pressure lube oil
- ✓ Anti motoring

During operation of the Class 1E GTG under a LOCA condition, all protective functions are bypassed except for “Overspeed”, “Generator differential current” and “High exhaust gas temperature”.

GTG System(1) *Class 1E GTG*

US-APWR

THE FEATURE OF GPS GAS TURBINE

1. No cooling water is required.
2. Easy to reduce the noise level (sound power level)
3. Less vibration
4. High seismic resistance
5. High reliability of starting
6. Less maintenance
7. High stability of the voltage frequency
8. Compact installation
9. Clean emission

GTG System(2) *Class 1E GTG*

US-APWR

GPS6000 Standard Specification

Item	Unit	Specification
Electrical Output (at 104 ° F)	**kW**	*4,800*
Allowable Ambient Temperature	**° F**	*41 – 104*
Starting Time	**Sec**	*Within 40.0*
Load Application Capacity	**%**	*100.0*
Frequency Deviation (Transient / Steady State)	**%**	*Within ±6.0 / ±0.3*
Fuel Type		*Kerosene / Diesel Oil / Heavy Oil*
Fuel Consumption (Kerosene / Diesel Oil / Heavy Oil)	**Gal / Hour**	*570.6 / 541.6 / 533.6*
Noise Level at 1m from Package	**dB(A)**	*85*
Noise Level at 1m from Exhaust Silencer Outlet	**dB(A)**	*90*
Gas Turbine Intake Air Flow Rate	**CFM**	*49,440*
Gas Turbine Exhaust Gas Flow Rate (at EGT 1103° F)	**CFM**	*135,255*
Ventilation Intake Air Flow Rate	**CFM**	*31,783*

GTG System(3) *Class 1E GTG*

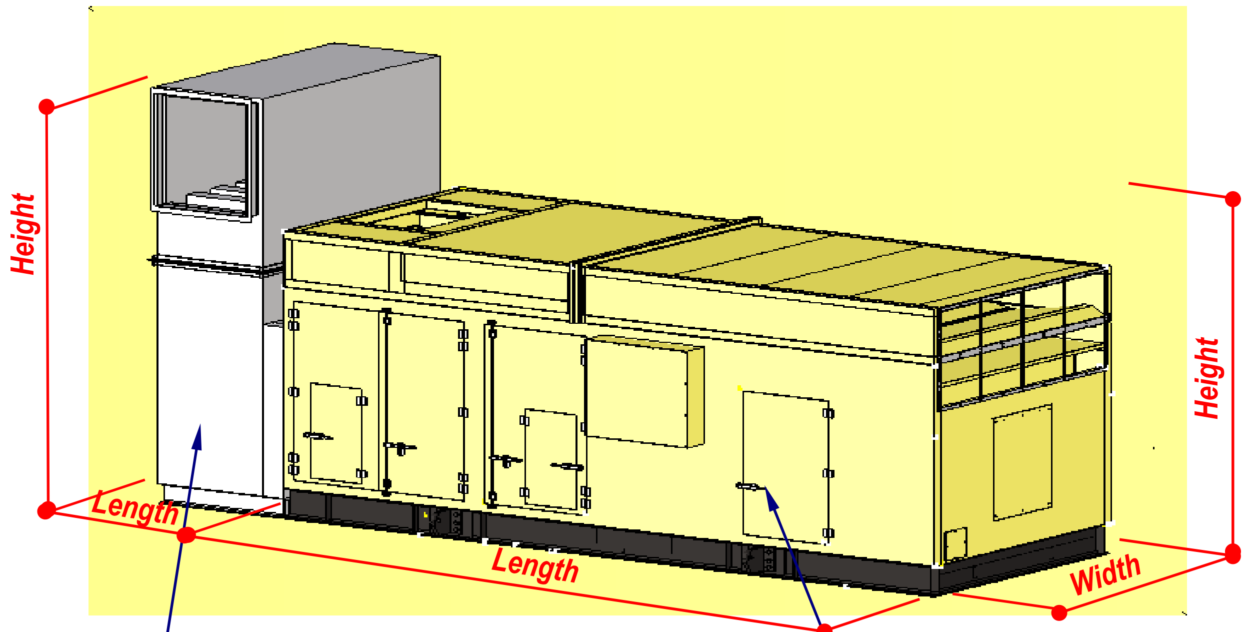
US-APWR

M1T—33 Gas Turbine Standard Specification

Item	Unit	Specification
Turbine Model		*Kawasaki M1T-33*
Engine Type		*Heavy-duty, Single-shaft Simple Open Cycle*
Compressor Type		*2-Stage Centrifugal*
Combustor Type		*Single Can*
Turbine Type		*3-Stage Axial*
Reduction Gear Box		*Planetary + Parallel*
Turbine Speed	**rpm**	*18,000*
Output Speed	**rpm**	*1,500 / 1,800*
Rated Power Output (at 40 ℃)	**kW**	*5,200*
Dry Weight	**Lb (kg)**	*29,762 (13,500)*
Recommended Lubricating Oil Type / Brand		*Synthetic Oil* *Shell ASTO500 / Mobil Jet2 / Castrol AERO5000 / BP BPTO2380*
Lubricating Oil Tank Capacity	**Gal**	*95.1*
Lubricating Oil Consumption	**Gal / Hour**	*0.053*

GTG System(4) *Class 1E GTG*

Size



Exhaust Silencer

Length	ft (m)	4.92 (1,500)
Width	ft (m)	9.84 (3,000)
Height	ft (m)	15.75 (4,800)
Weight	lb (kg)	11,244 (5,100)

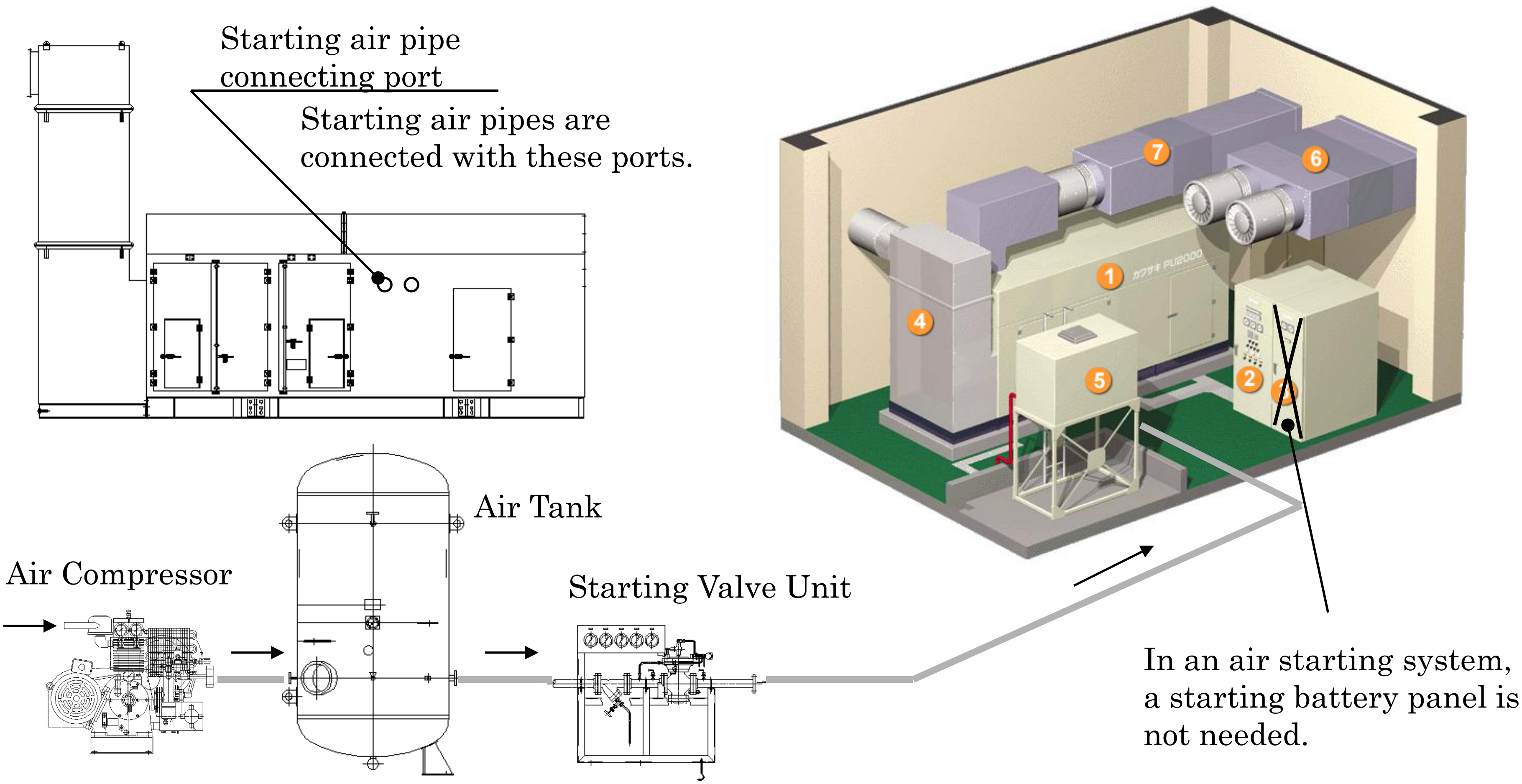
Gas Turbine Package

Length	ft (m)	25.26 (7,700)
Width	ft (m)	9.84 (3,000)
Height	ft (m)	11.81 (3,600)
Weight	lb (kg)	85,980 (39,000)

GPS6000 PACKAGE OUTLINE DIMENSIONS

GTG System(5) *Class 1E GTG*

Detail Design: Example, Air System



Important Input Parameter and Data to Safety analysis and PRA *Class 1E GTG*

Important input parameter and data to safety analysis and PRA are followings.

(1) Starting time: within 100 seconds

(2) Fuel storage tank: 7 days capacity per one train

(3) Reliability target are same as US nuclear EDGs.

Fail to Start

- Mean : 5.0×10^{-3} / demand
- 95%-tile : 1.5×10^{-2} / demand

Fail to Run

- mean : 8.0×10^{-4} / hr
- 95%-tile : 2.0×10^{-3} / hr

Above (1),(2) have already explained before. MHI shows the evaluation for “(3) Reliability” from next slide.

Reliability (1) *Class 1E GTG*

MHI's Reliability Verification Plan(1)

The reliability target of US-APWR Class 1E GTG is shown below. It is based on US EDG's data of NUREG-CR/6928. And this value is used to PRA analysis.

Fail to Start

- Mean : 5.0 × 10^{-3} / demand
- 95%-tile : 1.5 × 10^{-2} / demand

Fail to Run

- mean : 8.0 × 10^{-4} / hr
- 95%-tile : 2.0 × 10^{-3} / hr

Reliability (2) *Class 1E GTG*

US-APWR

MHI's Reliability Verification Plan(2)

MHI shows GPS6000 satisfies with reliability target of US-APWR using Bayesian approach.

First estimate of GPS6000 reliability performed by updating the non-informative prior (Jeffers's prior) with GPS's operational data.

(note)

Bayesian approach is one of general method of statistics, and is widely used to evaluate component reliability and its uncertainty.

NUREG-CR/6928 also uses this approach. Recognized in ASME PRA standard as preferred method for component data uncertainty analysis

Reliability (3) *Class 1E GTG*

MHI's Reliability Verification Plan(3)

In order to estimate GPS6000's reliability accurately, collection of data based on appropriate categorization is necessary.

MHI has analyzed available and relevant GPS's operational data.

Operational data has been collected from manufacture's records as shown in Table-1.

Reliability (4) *Class 1E GTG*

US-APWR

MHI's Reliability Verification Plan(4)

Table-1(1/2)

Product	Output(kVA)	Single engine or Twin engine	Fuel Type	Starting system	Failure/Number of starts	Failure/Operation hours
1	2000	Twin	Heavy Oil	Air	0 /251 d	0 /98 hr
2	2000	Twin	Heavy Oil	DC	0 /265 d	0 /75.4 hr
3	2000	Twin	Diesel Oil	DC	0 /100 d	0 /71.3 hr
4	2000	Twin	Kerosene	DC	0 /1053 d	0 /205 hr
5	2500	Twin	Heavy Oil	Air	0 /383 d	0 /1129.8 hr
6	2500	Twin	Heavy Oil	DC	0 /95 d	0 /16.4 hr
7	4000	Twin	Heavy Oil	Air	0 /540 d	0 /982 hr
8	4000	Twin	Heavy Oil	DC	0 /149 d	0 /96.8 hr
9	4000	Twin	Diesel Oil	Air	0 /225 d	0 /156.4 hr
10	4000	Twin	Diesel Oil	DC	0 /105 d	0 /50.8 hr
11	4000	Twin	Kerosene	DC	0 /263 d	0 /109.6 hr

Reliability (5) *Class 1E GTG*

US-APWR

MHI's Reliability Verification Plan(5)

Table-1(2/2)

Product	Output(kVA)	Single engine or Twin engine	Fuel Type	Starting system	Failure/Number of starts	Failure/Operation hours
12	4500	Twin	Heavy Oil	Air	0 /327 d	0 /125.1 hr
13	4500	Twin	Heavy Oil	DC	0 /130 d	0 /63.2 hr
14	4500	Twin	Diesel Oil	DC	0 /69 d	0 /80.3 hr
15	4500	Twin	Diesel Oil	DC	0 /147 d	0 /32.1 hr
16	4500	Twin	Kerosene	Air	0 /341 d	0 /455.1 hr
17	4500	Twin	Kerosene	DC	0 /251 d	0 /68.0 hr
18	5000	Twin	Unidentified	DC	0 /48 d	Operation period of those products are short. These are not used for evaluation as conservative.
19	5000	Twin	Unidentified	DC	0 /48 d	
20	6000	Twin	Unidentified	DC	0 /24 d	
21	6000	Twin	Unidentified	DC	0 /24 d	
22	6000	Twin	Unidentified	DC	0 /13 d	
23	6000	Twin	Unidentified	DC	0 /13 d	
24	6000	Twin	Unidentified	DC	0 /12 d	
25	6000	Twin	Unidentified	DC	0 /12 d	
26	6000	Twin	Unidentified	DC	0 /6 d	
27	6000	Twin	Unidentified	DC	0 /1 d	

Reliability (6) *Class 1E GTG*

US-APWR

MHI's Reliability Verification Plan(6)

➢ **Data collection of GTG fail to start**

1. GPS series have been produced with common design concept such as structure, dynamic characteristics and materials. Increasing of output is achieved to size up the design of small product analogously. Near output products have more similar design. MHI apply GPS6000 as EPS. GPS5000 is similar design as GPS6000. Also, GPS4000/4500 are almost similar design as GPS6000, and these are no significant difference of starting capability based on operation experiences. Another mean of increasing of output is using two engines with one generator. Over GPS 2000 products are twin type all.

2. Starting type is also considered whether air or DC motor.

Reliability (7) *Class 1E GTG*

US-APWR

MHI's Reliability Verification Plan(7)

➢ **Data collection of GTG fail to start (continued)**

3. MHI has selected the data of Table-1 as follow;

   - Data of GPS4000 to 6000 with air starting type

     ⇒ 1433 demands with 0 failure

This data is used to Bayesian approach of GTG reliability.

Reliability (8) *Class 1E GTG*

MHI's Reliability Verification Plan(8)

➢ Data collection of GTG fail to run

From view point of running reliability, type of starting system is not needed to consider. Also, there are no significant difference from operation experiences of large output twin engine products of over GPS2000. MHI has classified data into running time of over GPS2000 and running time over GPS4000.

1) Data of over GPS2000 ⇒ 3820 hours with 0 failure

2) Data of over GPS4000 ⇒ 2224 hours with 0 failure

Result of this, MHI evaluates both above 1) and 2) are considered proper to use to Bayesian approach. However, MHI evaluates using only data of 2) conservatively.

Reliability (9) *Class 1E GTG*

MHI's Reliability Verification Plan(9)

➢ **Reliability estimation of GTGs based on industry operational experience**

✓ **Applicable data**

- 1433 demands with 0 failure
- 2224 run hours with 0 failure

✓ **Uncertainty of failure rate/probability**

- Estimated by posterior distribution of Bayesian approach

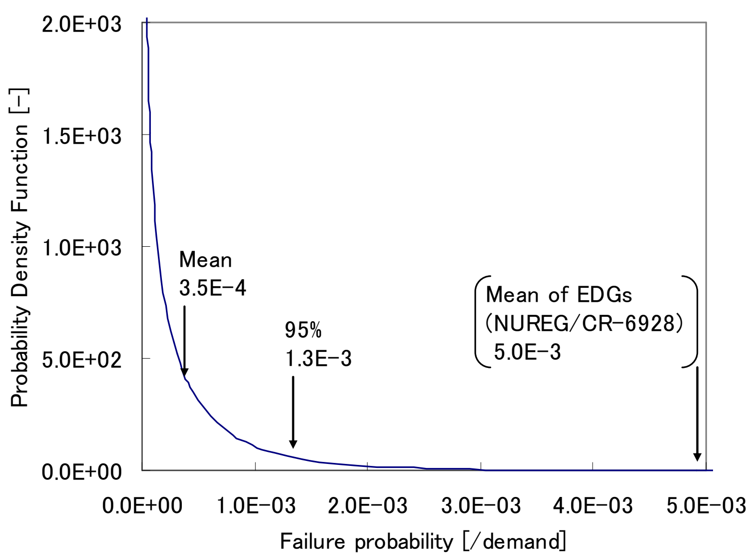
Table-2

	5%	Mean	95%	Distribution		
				Type	α	β
Fail to start	1.4E-6	3.5E-4	1.3E-3	Beta	0.5	1433
Fail to run	8.9E-7	2.2E-4	8.3E-4	Gamma	0.5	2224

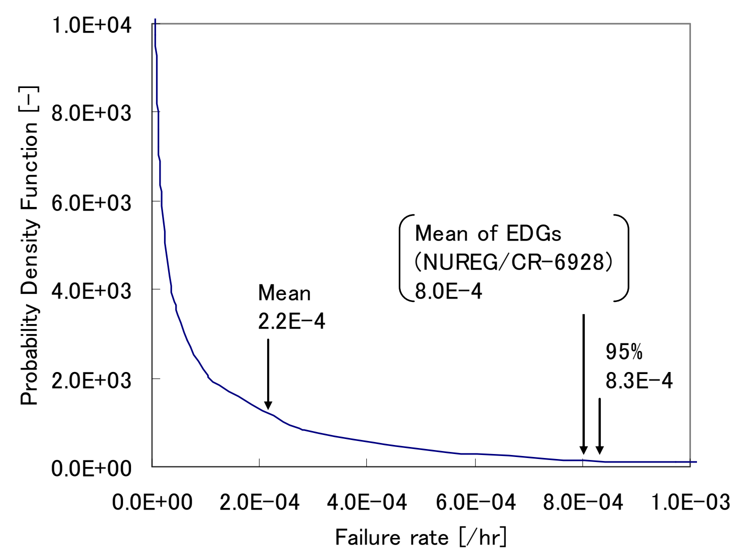
Reliability (10) *Class 1E GTG*

MHI's Reliability Verification Plan(10)

Posterior distribution of GTGs reliability



Fail to start



Fail to run

Reliability (11) *Class 1E GTG*

MHI's Reliability Verification Plan(11)

➢ US-APWR GTG test plan

✓ **Start test**

- Operational experience show that failure rate is lower than the mean failure rate of DGs (5.0E-3 /d), with 95% confidence.
- Start tests will be performed as a typical "qualification starting test". Total starting times is 100.
- Reliability will be updated by the starting test and surveillance test results obtained during plant operation

✓ **Run test**

- Operational experience show that failure rate is lower than the mean failure rate of DGs (8.0E-4 /hr), with approximately 95% confidence.
- Run test is not needed.
- Reliability will be confirmed and updated by surveillance test results obtained during plant operation

Table-3 GTG unreliability given start test results

Start Test results		Estimated US-APWR GTG reliability		
Trials	failures	5%	Mean	95%
100	0	1.3E-6	3.3E-4	1.3E-3

Reliability (12) *Class 1E GTG*

US-APWR

MHI's Reliability Verification Plan(12)

- Based on limited test data, GTG reliability appears to be capable of exceeding reliability assumed in PRA.
- In addition to MHI's PRA reliability target, MHI should satisfy with reliability requirement of R.G 1.155. R.G 1.155 requires over 0.95 or 0.975 reliability with 95% confidence.

  Target case of 0.95: 100 start up test

  Target case of 0.975: 150 start up test
- Future operating experience will be needed to demonstrate that reliability targets can be achieved and maintained over the life of the plant. MHI will update the GTG reliability during operation through surveillance tests.

Class 1E Qualification (1) *Class 1E GTG*

US-APWR

- *Plan of Class 1E Qualification*

  The GTG shall meet the same requirements for the Emergency Diesel Generator, complying with Regulatory Guide 1.9 Rev. 4 and IEEE-387.The qualification process will be completed by the end of 2010.

  ✓ The Commercial Grade Item (CGI) dedication process will be used for the Qualification procedure, per EPRI NP 5652 endorsed by NRC GL 91-05. These guidelines will be applied to the procurement, acceptance, testing and Class 1E dedication of the GTG.

  ✓ Procedure

  Testing will be performed per IEEE 387 and Regulatory Guide 1.9 Rev. 4

  ✓ Seismic Qualification

  Seismic Analysis per IEEE 344

Develop Dedication Report

- Identify Form, Fit, and Function
- Failure Mode Analysis
  - ✓ Effect of part failure on System
  - ✓ Credible Failure Modes of Part
- Design Information
  - ✓ Catalog Information
  - ✓ Manufacturer's Drawings, etc.
- Critical Characteristics
  - ✓ Dimensions
  - ✓ Operability
  - ✓ Material

US-APWR

Develop Dedication Report (continued)

- **Environmental Qualification**
  - ✓ Manufacturer's specs
  - ✓ Environmental chamber
- **Seismic Qualification**
  - ✓ Perform an analysis
  - ✓ Write seismic (shake) test procedure
- **Shelf Life**
  - ✓ Identify materials
  - ✓ Utilize published standards
- **Maintenance / Surveillance / Replacement Interval**
  - ✓ Activity required by customer to maintain qualification
- **Verify operability**
  - ✓ Write functional test procedure

Class 1E Qualification (4) *Class 1E GTG*

US-APWR

- Qualification Testing - IEEE-387 (1995) and US NRC RG1.9
- Factory Acceptance Testing
  - ✓ Engine Test
    - Load Test at Factory
  - ✓ Generator Test
    - NEMA MG-1 at Factory
  - ✓ Combined Unit Test (at Factory)
    - Initial Operation and Load Test
    - Excitation & Controls Test
    - Alarm Verification
    - Start Time & Receiver Capacity
    - Protective Trip Bypass
    - Test Mode Override

Class 1E Qualification (5) *Class 1E GTG*

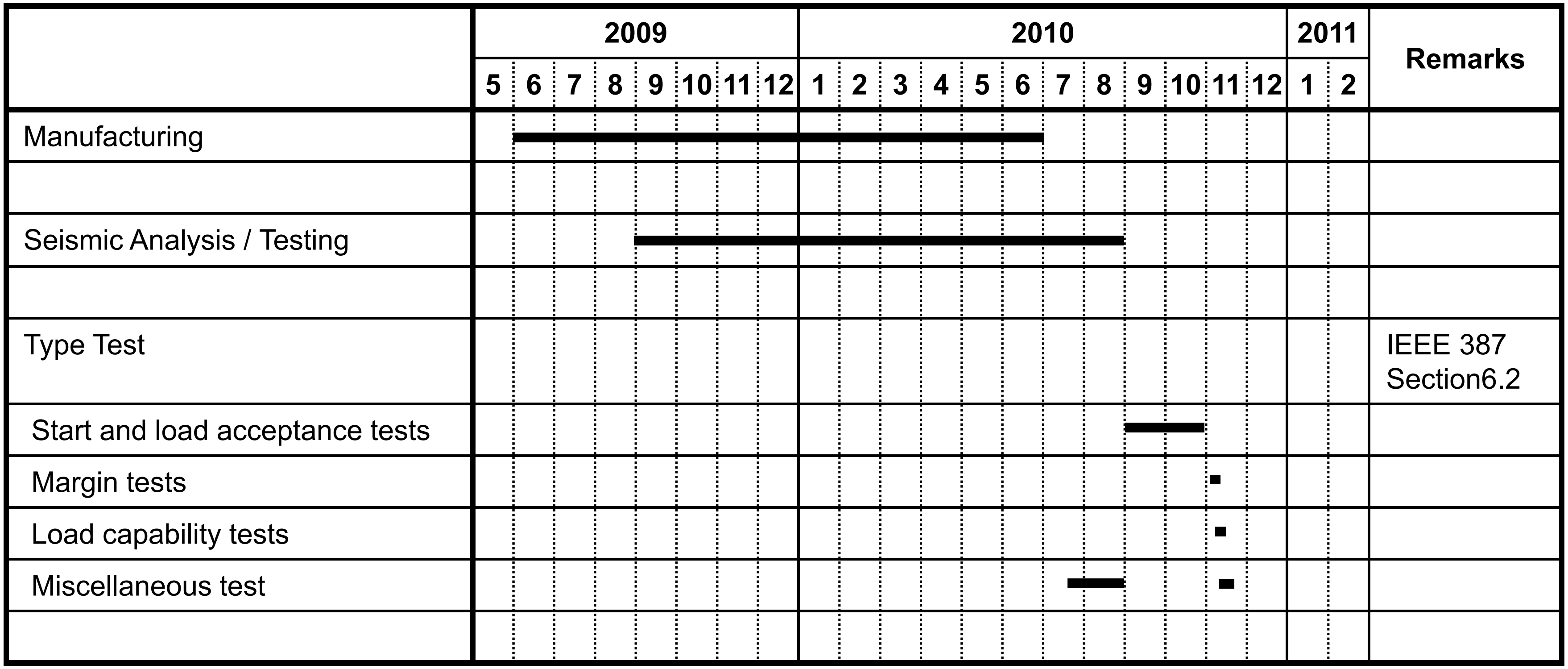
US-APWR

- **Type Test**
  - ✓ **Load capability tests**
    - 24-Hour Load Test
    - 110% Load Rejection Test
  - ✓ **Start and load acceptance tests**
    - 100 Start and Load Reliability Test
  - ✓ **Margin tests**
    - 110% of most severe load step

Class 1E Qualification (6) *Class 1E GTG*

US-APWR

➢ Class 1E Qualification Schedule



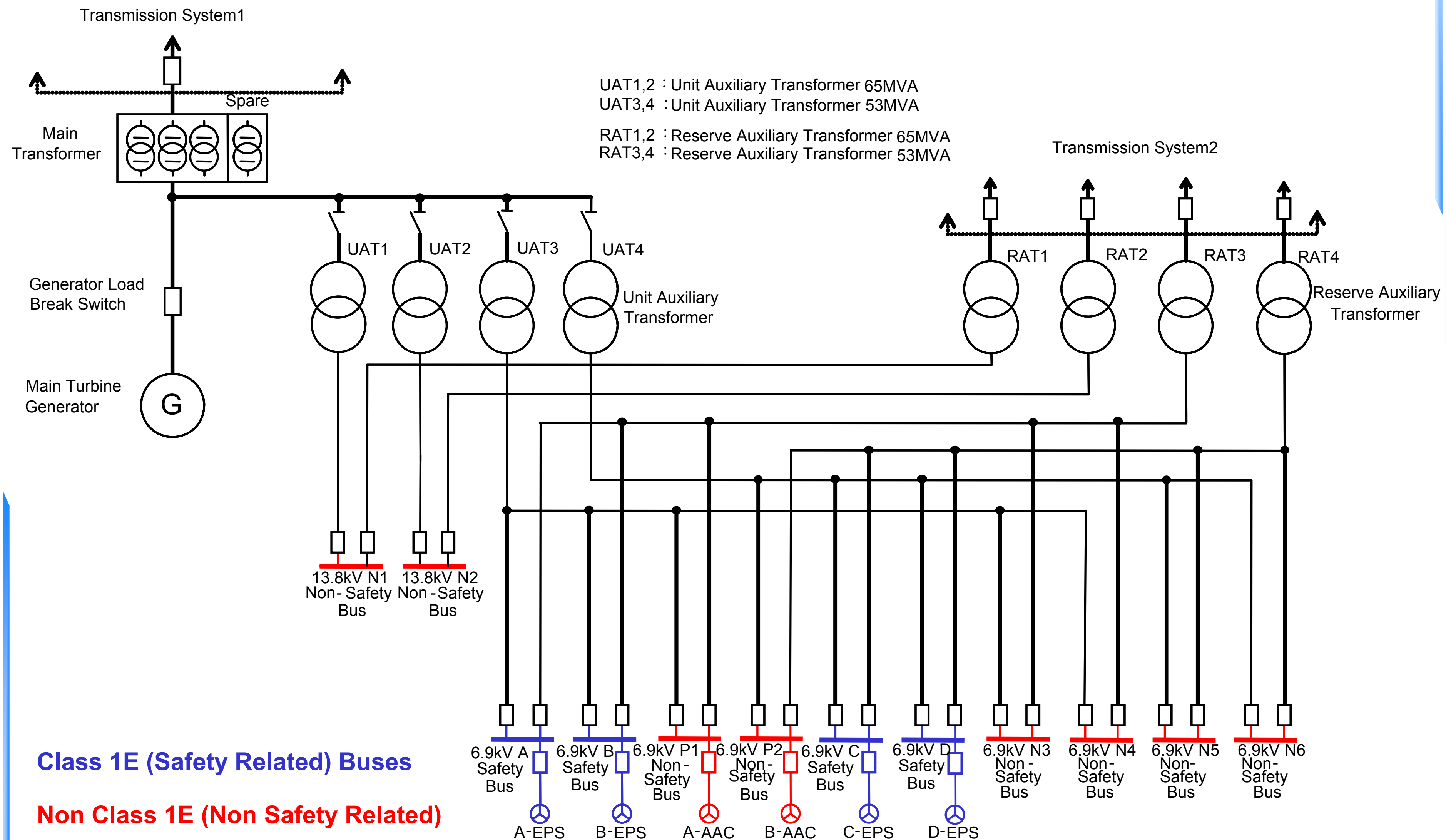
Introduction *AAC-GTG*

- The alternate AC power sources (AAC) are available in the event of a station blackout (SBO), when all offsite power sources and Class 1E GTGs are not available to bring the unit to a safe shutdown condition and maintain that status.

- US-APWR has two AAC power sources which apply non safety-related Gas Turbine Generators.

Onsite AC Power System *AAC-GTG*

➢System Configuration



Class 1E (Safety Related) Buses

Non Class 1E (Non Safety Related) Buses

Design Basis of AAC-GTG *AAC-GTG*

- *Design Basis*
  - ✓ AAC-GTG of a different type (Starting System, Capacity etc,) is provided to minimize the potential for common mode failure with either the offsite power or the Class 1E GTG system
  - ✓ The AAC-GTG is a non-class 1E engine-generator package connected to a 6.9kV AC “permanent” bus.
  - ✓ The AAC-GTG supplies power to loads of a class 1E bus through the tie line circuit during SBO.
  - ✓ The AAC-GTG supplies power to loads for 8 hours during SBO.
  - ✓ The AAC-GTG system to be designed having diversity from Class 1E GTG system.

Requirement, Design concept and Specification *AAC-GTG*

➢ Design requirement, Specification of AAC-GTG

- ✓ Non safety-related, non Class 1E
- ✓ Two units
- ✓ 4000 kW Continuous
- ✓ 6900 V, 3-phase, 60 Hz
- ✓ DC motor starting type
- ✓ Fuel: Diesel oil, fuel storage tank of each train has capability to operate the GTG during seven days under continuous rated capacity. Fuel day tank of each train has capability to operate the GTG during 1.5 hours under continuous rated capacity.

Power Supply to Onsite Buses *AAC-GTG*

- *Permanent Buses*
  - ✓ There are two buses for exclusive use for each AAC.
  - ✓ In LOOP condition, non-safety loads required are supplied via the "permanent" bus from AAC.

	Normal Operation	*LOOP*	*SBO*
Class 1E Buses	*RAT*	*EPS*	*AAC*
Non safety-related "Permanent" Buses	*UAT*	*AAC*	*AAC (Only Required Loads)*

Operation under the SBO(1) *AAC-GTG*

- *Definition of SBO*

  - ✓ SBO refers to the complete loss of alternate current electric power to the essential and nonessential switchgear buses.

  - ✓ SBO therefore involves the loss of offsite power concurrent with turbine trip and failure of onsite emergency ac power system (4 trains, 4 Class 1E emergency generators), but not the loss of available ac power to buses fed by station batteries through inverters or the loss of power from “alternate ac sources”.

Operation under the SBO(2) *AAC-GTG*

US-APWR

- *Basic Concept against for SBO*

SBO occurs

The all offsite power and four EPSs will be lost. But two alternate AC power sources (AACs) and batteries will be still available.

Switching of buses and starting loads

Tie-line between permanent MV bus and safety MV bus will be connected.
And needed loads (safety loads and non-safety loads) are re-operated.
All operations can be achieved within one hour.

Plant Target and Safety

Plant can keep the integrity of components and safety condition (e.g. integrity of RCP seal) until completion of switching buses and re-starting loads. And after this, Plant can keep the Hot-Standby condition for 7 days without AAC fuel supply from offsite.

Operation under the SBO(3) *AAC-GTG*

US-APWR

➢ AAC-GTG backup Power Supply to Class 1E buses

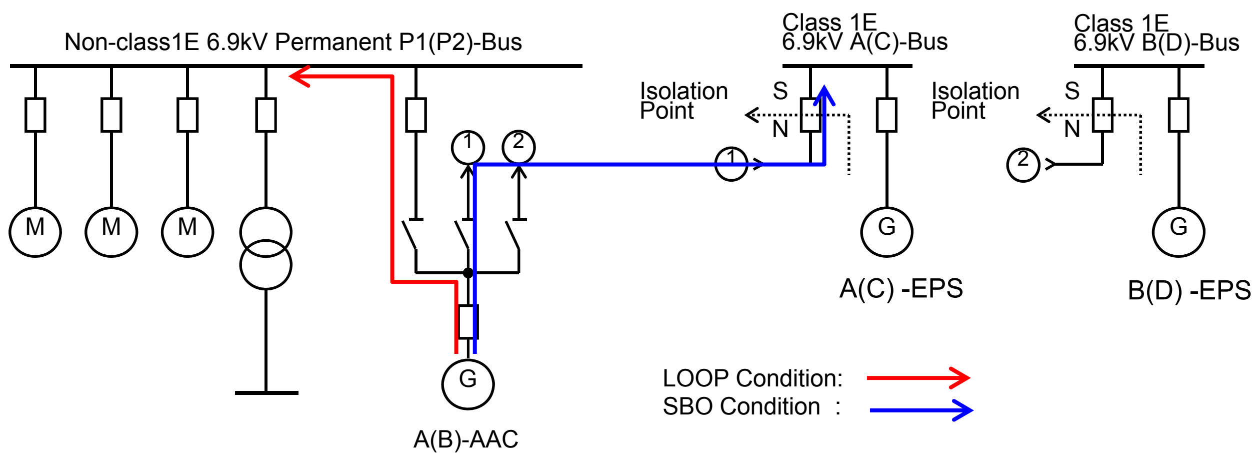
When a SBO occurs, the AAC power source supplies power to any of the selected safety division in accordance with the following procedure:

1) Switching will be done manually to prevent starting loads on any other division.

2) Loads that need to be stopped on the "permanent" bus will be tripped manually.

3) The required breaker to the back-up division will be closed manually.

4) Back-up bus will be energized and loaded as necessary for coping with SBO. The loads will be started manually.



Operation under the SBO(4) *AAC-GTG*

US-APWR

- *Operation of Plant under the SBO Condition*

Function	*Main Features*
Reactivity Control	*Boric Acid Pump* ***(1 pump)***
Supply of RCS water	*Charging Pump* ***(1 pump)***
Control of RCS pressure	*Pressurizer Backup Heater* ***(1 train)***
Remove of decay heat	*Main Steam Relief Valve,* *Turbine Driven EFWP* ***(1 pump)***
Cooling of RCP seal	*Charging Pump* ***(1 pump)***
Supporting System	*ESWP* ***(1 pump)****, CCWP* ***(1 pump)*** *Containment Service Water Cooling Tower Fans* ***(1 train)*** *Chiller Unit, HVAC, Battery Charger, AAC supporting components, UPS unit, Instrument and Control Cabinets etc.*

(   );Required Minimum Quantity

Operation under the SBO(5) ***AAC-GTG***

➢ Evaluation

- ✓ Starting time of AAC is within 100 seconds after SBO occurs. Reenergize of bus by AAC and restarting of loads will be completed within one hour after SBO occurs.
- ✓ Plant can keep safety condition until completion of reenergize by AAC and restarting loads. RCP seal can be kept the integrity for 8 hours without cooling.
- ✓ Plant can keep safety and Hot Standby condition with only one AAC, one permanent division (and loads) and one Class 1E division (and loads) for 7 days.

Diversity(1) *AAC-GTG*

Diversity between EPS and AAC

- AAC-GTG should be designed to minimize the potential of common cause failure with safety-related EPS system. Diversity between design of Class 1E GTG system and AAC-GTG system is preferable.

- MHI is now under proceeding following two approach.
  1. Different Manufactures/Products
     : Design issue on diversity on between Class 1E GTG and AAC-GTG is clearly resolved by itself.
  2. Same Manufacture
     : Design issue on diversity is resolved by using analysis such as evaluation for eliminating CCF.

- MHI shows one approach of evaluation CCF from next slide.

Diversity(2) *AAC-GTG*

Detail of diversity between EPS and AAC(1)

- US-APWR applies GPS6000 as EPS, GPS5000 as AAC. Design and specification of these engine portion are almost similar. Table-5 shows detail differences between whole GTG system component and design between both systems.
- Each item of engine portion of both are almost similar. However, difference of output means difference of combustion rate, also dynamic characteristics of both are different. This deference effects to decrease the CCF potential.
- Also, there are many differences of spec., design and manufacture for supporting system component.

Diversity(3) *AAC-GTG*

US-APWR

Detail of diversity between EPS and AAC(2)

- As explained, design and specification of both engine portions are almost similar. However, NRC's report (discussed on "Reliability"), evaluates the cause and portion of failures.
- According to NRC report, cause and portion of failures of FY1998 to FY2007 has been researched as Table-4.

Table-4

Fail to start Total:116 failures		Fail to Run Total:65 failures	
Lank	Portion	Lank	Portion
1	I&C : 34 failures	1	Cooling : 15 failures
2	Generator : 23 failures	2	Engine : 12 failures
3	Starting air : 13 failures	3	Fuel oil : 11 failures
4	Governor: 12 failures	4	I&C : 9 failures
5	Fuel oil: 10 failures	5	Lube oil : 8 failures
6	cooling: 10 failures	6	Generator : 6 failures
8	Engine: 4 failures		

Diversity(4) *AAC-GTG*

Detail of diversity between EPS and AAC(3)

- According to Table-4, failure caused by engine are considered low probability. GPS6000 and GPS5000 planed to US-APWR are designed different supporting system including starting system.

  Based on this fact, Fail to Start caused by engine are considered low probability.

- In addition, GPS6000 and GPS5000 are designed different output, combustion rate. This different is expected to prevent the Fail to Run.

- MHI considers although GPS6000 and GPS5000 are similar engine design, it is expected to minimize the CCF potential view point both of start and run availability.

Diversity(5) *AAC-GTG*

US-APWR

Detail of diversity between EPS and AAC(4)

Table-5(1/3)

Group	No	Item	EPS	AAC
Engine	1	Type	M1T-33	M1T-33A
	2	Rated output (engine edge)	5200kW	4362kW
	3	Combustor spec/material/size	Single CAN Type/heat-resistant alloy	Same as follows
	4	Number of turbine blades /rows	1st row = 44 2nd row = 40 3rd row = 36	Same as follows
	5	Turbine engine spec/material/size	3-Stage Axial / nickel-based heat-resisting alloys	Same as follows
	6	Compressor spec/material/size	2-Stage Centrifugal / titanium alloy	Same as follows
	7	Number of compressor blade rows	Total 54	Same as follows
	8	Compressor compression ratio	10.23	10.08
	9	Exhaust gas temperature	595 degree C	540 degree C
	10	Exhaust gas flow	3830 m^3/min	3650 m^3/min
	11	Gear spec/material/size	Planetary + Parallel	Same as follows
	12	Change gear ratio	10:1	Same as follows

Diversity(6) *AAC-GTG*

Detail of diversity between EPS and AAC(5)

Table-5(2/3)

Group	No	Item	EPS	AAC
Supporting system Equipment installed on Engine	13	Starting Motor type	Air	DC motor
	14	Starting Motor quantity	4	8
	15	Starting Motor spec	Air Turbines x 4	40kW DC60V Motors x 8
	16	Main fuel pump (shaft driven) spec/quantity	screw type 23L/min @3.3MPa x 2	Potentially change manufacture
	17	Starting fuel pump (shaft driven) spec/quantity	Gear type x 2	Potentially change manufacture
	18	Starting fuel pump (DC motor driven)	DC24V gear type x 2	Potentially change manufacture
	19	Fuel control valve spec/quantity	Electric type x 2	Potentially change manufacture
	20	Main lube oil pump spec/quantity	Gear type x 2	Potentially change manufacture
	21	Pressure control valve spec/quantity	Plunger type x 2	Potentially change manufacture
	22	Ignition plug spec/quantity	surface gap type x 4	Potentially change manufacture
	23	Governor spec/quantity	Electric type x 2	Potentially change manufacture
Design control, Engineering, manufacturing	24	Designing/ manufacturing manual	Specified for MIT-33	Specified for MIT-33A
	25	Quality control department	Base with ESI	Base (without ESI)
	26	Manufacturing line	Base	Same with Base

Diversity(7) *AAC-GTG*

Detail of diversity between EPS and AAC(6)

Table-5(3/3)

Group	No	Item	EPS	AAC
GTG system supporting component	27	Fuel oil transfer pump	Safety-related	Non safety-related, different manufacture, different spec.
	28	Starting air valve	Safety-related	N/A
	29	Fuel day tank	Safety-related	Non safety-related, different manufacture, different spec.
	30	Fuel storage tank	Safety-related	Non safety-related, different manufacture, different spec.
	31	Fuel system piping	Safety-related	Non safety-related, different manufacture, different spec.
	32	Exhaust duct	Safety-related	Non safety-related, different manufacture, different spec.
	33	Inlet duct	Safety-related	Non safety-related, different manufacture, different spec.
	34	Ventilation fan	Safety-related	Non safety-related, different manufacture, different spec.
	35	Generator	Class 1E	Non Class 1E, different manufacture, different spec.
	36	Generator excitation circuit	Class 1E	Non Class 1E, different manufacture, different spec.
	37	AVR	Class 1E	Non Class 1E
	38	GTG control panel (hardwired)	Class 1E	Non Class 1E, different manufacture
	39	GTG control panel (DDC)	Class 1E	Non Class 1E, different manufacture
	40	AC power supply	Class 1E bus	Non Class 1E bus
	41	DC power supply	Class 1E bus	Non Class 1E bus